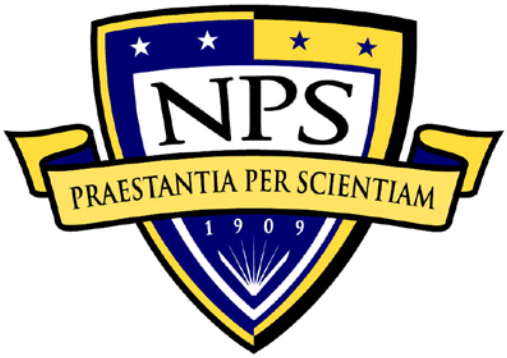


# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**SAUDI ARABIA'S COUNTERTERRORISM METHODS: A CASE STUDY ON HOMELAND SECURITY**

by

Majed M. Bin Madhian

June 2017

Thesis Advisor: James Russell
Co-Advisor: Scott Jasper

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|



| 1. AGENCY USE ONLY *(Leave blank)* | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | June 2017 | Master's thesis |

**4. TITLE AND SUBTITLE**
SAUDI ARABIA'S COUNTERTERRORISM METHODS: A CASE STUDY ON HOMELAND SECURITY

**5. FUNDING NUMBERS**

**6. AUTHOR(S)** Majed M. Bin Madhian

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Naval Postgraduate School
Monterey, CA 93943-5000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
N/A

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release. Distribution is unlimited.

**12b. DISTRIBUTION CODE**

**13. ABSTRACT**

This thesis is a case study on counterterrorism methods. Specifically, it examines Saudi Arabia's multidimensional counterterrorism measures to combat the Islamic State's aggressions and threats. After deriving a theoretical framework based on counterterrorism measures developed from a review of scholarly literature, the thesis presents three questions. By comparing examples from the case study to the hypotheses, the thesis finds that Saudi Arabia effectively implements a multidimensional approach consisting of legal, financial, and informational methods to respond to the Islamic State's threats. In addition to enacting stricter criminal laws and enforcement of those laws to safeguard the homeland and its borders, Saudi Arabia has enacted laws that impose stiff penalties aimed at money laundering and other illicit activities that fund terrorist activity. Finally, the Kingdom has implemented stringent cybersecurity measures not only to prevent hacking of Saudi cyberspace by terrorists, but also to monitor the Islamic State's communications. Beyond these conventional and punitive measures, Saudi Arabia has implemented successful "soft" measures, including an innovative rehabilitation program. Based upon these findings, the study recommends Saudi Arabia expand its countermeasures by placing economic sanctions on the Islamic State and its supporters. Further recommendations direct policymakers to consider military intervention and regime change in Syria, and to destroy the Islamic State's infrastructure.

**14. SUBJECT TERMS**
Saudi Arabia, counterterrorism, rehabilitation center, soft power, Islamic State

**15. NUMBER OF PAGES**
87

**16. PRICE CODE**

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UU |

NSN 7540-01-280-5500
Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release. Distribution is unlimited.**

# SAUDI ARABIA'S COUNTERTERRORISM METHODS: A CASE STUDY ON HOMELAND SECURITY

Majed M. Bin Madhian
Major, Saudi Arabia National Guards
B.S., King Khalid Military College, 2001

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(STRATEGIC STUDIES)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2017**

Approved by: James Russell
Thesis Advisor

Scott Jasper
Co-Advisor

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

This thesis is a case study on counterterrorism methods. Specifically, it examines Saudi Arabia's multidimensional counterterrorism measures to combat the Islamic State's aggressions and threats. After deriving a theoretical framework based on counterterrorism measures developed from a review of scholarly literature, the thesis presents three questions. By comparing examples from the case study to the hypotheses, the thesis finds that Saudi Arabia effectively implements a multidimensional approach consisting of legal, financial, and informational methods to respond to the Islamic State's threats. In addition to enacting stricter criminal laws and enforcement of those laws to safeguard the homeland and its borders, Saudi Arabia has enacted laws that impose stiff penalties aimed at money laundering and other illicit activities that fund terrorist activity. Finally, the Kingdom has implemented stringent cybersecurity measures not only to prevent hacking of Saudi cyberspace by terrorists, but also to monitor the Islamic State's communications. Beyond these conventional and punitive measures, Saudi Arabia has implemented successful "soft" measures, including an innovative rehabilitation program. Based upon these findings, the study recommends Saudi Arabia expand its countermeasures by placing economic sanctions on the Islamic State and its supporters. Further recommendations direct policymakers to consider military intervention and regime change in Syria, and to destroy the Islamic State's infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| DCPP | Defense Cyber Protection Partnership |
| FATF | The Financial Action Task Force |
| IDC | International Data Corporation |
| ISIL | Islamic State in Iraq and the Levantine |
| ISIS | Islamic State in Iraq and Syria |
| NCPP | National Cybersecurity Protection Plan |
| NCSP | National Cybersecurity System Program |
| NGO | non-governmental organization |
| SAMA | Saudi Arabia’s Monetary Agency |
| SCF | Strategic Cooperation Forum |
| UK | United Kingdom |
| UN | United Nations |
| U.S. | United States |

THIS PAGE INTENTIONALLY LEFT BLANK

# EXECUTIVE SUMMARY

Since 2003, the Kingdom of Saudi Arabia has been effectively responding to al-Qaeda's with conventional weapons and methods. Countering the Islamic State's, however, has required Saudi Arabia to transform is counterterrorism methods to include multidimensional tasks. Such tasks require the Kingdom to customize and expand their typical measures to combat the Islamic State's frequent attacks on Saudi soil. Beyond its borders, the Kingdom also strives hard to eliminate the Islamic State in Iraq and Syria, where Saudi nationals fighting for the Islamic State in Syria and Iraq represent the second largest group of foreign fighters. Many of these fighters frequently return to Saudi Arabia and launch deadly attacks against Saudi targets. Furthermore, as the holy land for all Muslims worldwide, the Kingdom is also a target for many non-Saudi national fighters, who enter the Kingdom allegedly for religious purposes and launch deadly attacks there.

As home to Mecca and Medina, Saudi Arabia represents the greatest strategic interest for the Islamic State, which hopes to gain legitimacy by occupying these holy cities. To foil the Islamic State's plans to gain legitimacy in this way, Saudi Arabia must implement a comprehensive and sophisticated response that relies on more than the typical mechanized weapons. Such a comprehensive and multidimensional response consists of legal, financial, and informational counterterrorism measures. Accordingly, this thesis poses three major research questions: what are the legal, financial, and informational counterterrorism measures that Saudi Arabia uses today to respond to Islamic State threats? What additional counterterrorism measures does Saudi Arabia need to implement to combat the Islamic State's threats going forward? What else does Saudi Arabia need to do to foil the Islamic State's plans?

The academic literature on counterterrorism presents deep insight into the Islamic State's strategic rationales and the appropriate measures to defeat the group. Nonetheless, there is still a need to provide Saudi Arabia and its partners

a better understanding of more effective counterterrorism methods to eliminate the notorious organization. Therefore, this study uses scholarly approaches for combating terrorism within a theoretical framework to examine comparatively Saudi Arabia's current measures and methods. Understanding how to improve these measures for combating terrorism will provide Saudi Arabia and its partners with the customized and effective tools to deliver a decisive defeat to the Islamic State.

To analyze and understand Saudi Arabia's measures for combating the Islamic State, the study proposes three answers to the major research questions derived from the theoretical framework of counterterrorism measures introduced in the review of the scholarly literature available on the topic. The findings from the comparison of the Kingdom's methods to the proposed answers show that in safeguarding the homeland and surveilling its borders and residential territories, Saudi Arabia implements strict criminal law enforcement to respond to the Islamic State's suicide and shooting incidents. Additionally, Saudi Arabia implements cyber-crime laws that address electronic crimes such as "credit card fraud, Internet crimes, cyber terrorism, creation and/or distribution of viruses, hacking, system interference, illegal access and interception."[1] Furthermore, Saudi Arabia implements strict banking laws to prevent terrorist fundraising to finance the Islamic State's operation.

Beyond these methods, the study also finds that Saudi Arabia pursues non-punitive efforts to rehabilitate citizens convicted of terrorism-related offenses. These programs aim to deter Saudis from involvement in radicalization, offer rehabilitation counseling and means, and provide aftercare programs to individuals involved in radicalization to "facilitate reintegration into society after their release from custody."[2] To defeat and eliminate the Islamic State totally the study suggests the following recommendations:

1. Saudi Arabia and its partners are strongly recommended to pursue heavy sanctions on Islamic State members and entities, and impose coercive penalties for individuals or states that are not fully

cooperative with the adopted UN Security Council Resolution 2199 calling upon “the member states to cut off the sources of ISIS financing."[3]

2. Saudi Arabia and its partners are strongly recommended to consider military intervention to bring about regime change in Syria.

3. Saudi Arabia and its partners are strongly recommended to pursue heavy attacks with ground troops, supported by airstrikes, to destroy the Islamic State’s infrastructure.

---

1. Bushra Mohamed Elamin Elnaim, “Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future,” *Information and Knowledge Management* (IISTE) 3, no. 13 (2013): 16, http://docplayer.net/15920297-Information-and-knowledge-management-issn-2224-5758-paper-issn-2224-896x-online-vol-3-no-12-2013.html.

2. Christopher Boucek, *Saudi Arabia’s “Soft” Counter-terrorism Strategy: Prevention, Rehabilitation, and Aftercare*, Carnegie Endowment for International Peace, Middle East Program, Report no. 97, September 2008, 4, http://carnegieendowment.org/files/cp97_boucek_saudi_final.pdf.

3. Laurence Bindner and Gabriel Poirot, "ISIS Financing 2015," Center for the Analysis of Terrorism, May 2015, 26, http://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

I am thankful to God on all occasions as I am nothing before Him, only a poor being whose deeds are submissive to His will and command whether awake or asleep. If I am to thank anybody on the face of this earth, I sincerely thank Professor James Russell and Professor Scott Jasper for carrying me patiently out of darkness to where there is light. I have traveled a very long, challenging journey, experiencing the risks of failure. I would have failed had my advisors, Professor Russell and Professor Jasper, not patiently stuck with me to succeed and accomplish writing my thesis. Their encouragement, criticisms, and insights have undoubtedly helped me to challenge all the difficulties I have faced through my journey. My extreme thanks are also extended to the National Security Affairs faculty and staff and to my classmates for their tremendous support. I will always appreciate and will never forget what they have done for me. My uncountable thanks are always offered to them wherever I live and as long as I live.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

The Kingdom of Saudi Arabia has been a constant target of terrorists' attacks for several decades, even though the Kingdom is countering these attacks with great efficiency. Given Saudi Arabia's success, terrorists should have abandoned their practice of targeting Saudi Arabia. Instead, attacks continue, requiring the Kingdom to increase its countermeasures, which presents the opportunity for a case study on how Saudi Arabia fights such terrorism. To undertake the case study, this thesis offers four chapters that examine Saudi Arabia's homeland security measures based on a theoretical frame developed from scholarly studies on counterterrorism, provide discussions and analysis of evidence, details findings on how Saudi Arabia fights terrorism, and makes recommendations on how to eliminate terrorism on the Kingdom's soil.

## A. MAJOR RESEARCH QUESTION

Terrorism has marked a serious homeland security threat across the Kingdom of Saudi Arabia.[1] Unlike al-Qaida's threats, which the Kingdom has been countering since 2003, Islamic State's threats have driven Saudi Arabia to transform its counterterrorism efforts into a multidimensional approach.[2] Such an approach requires the Kingdom to confront attacks not only on Saudi soil, but also to fight against the Islamic State in Iraq and Syria, from which the threats originate.[3] This is because Saudi nationals make up the second largest group of foreign fighters in Syria and Iraq. Many of these fighters frequently return to Saudi Arabia and launch deadly attacks against Saudi targets.[4] Moreover, as the holy land for all Muslims, the Kingdom is also a target for many non-Saudi

1 Daniel Byman, "The U.S.-Saudi Arabia Counterterrorism Relationship," prepared testimony, Brookings, May 24, 2016, 3, https://www.brookings.edu/wp-content/uploads/2016/07/Byman-Saudi-Arabia-HFAC.pdf.

2 Byman, "The U.S.-Saudi Arabia Counterterrorism Relationship," 4.

3 Ibid., 4, 5.

4 Aaron Y. Zelin, The Saudi Foreign Fighter Presence in Syria,report no. V. 7, Issue 4, April 2014, 13, https://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20140428-CTCSentinel.pdf.

national fighters who enter the Kingdom allegedly for religious purposes and launch deadly attacks there.[5]

Although the Islamic State makes serious efforts to expand globally, the Kingdom seems to represent the greatest strategic interest for the Caliphate. Following such interest, the Caliphate refers to Saudi Arabia as Wilayat al Haramayn, which means the Province of the Two Holy Places, referring to the Islamic holy sites of Mecca and Medina.[6] Occupying Mecca and Medina seems a priority for the Islamic State to gain legitimacy. To foil the Islamic State's plans to gain legitimacy in this way, Saudi Arabia must implement a comprehensive and sophisticated response that relies on more than the typical mechanized weapons. Such a comprehensive and multidimensional response consists of legal, financial, and informational counterterrorism measures. Accordingly, this thesis poses three major research questions: what are the legal, financial, and informational counterterrorism measures that Saudi Arabia uses today to respond to Islamic State threats? What additional counterterrorism measures does Saudi Arabia need to implement to combat the Islamic State's threats going forward? What else does Saudi Arabia need to do to foil the Islamic State's plans?

## B. POTENTIAL EXPLANATIONS AND HYPOTHESES

To answer the major research questions, this study reviews the scholarly literature on the topic and hypothesizes about the several methods Saudi Arabia employs to fight the increasing number of terrorist threats on its soil. These hypotheses are based on the methods adopted by other countries, such as the United States and the United Kingdom, that have been impacted by terrorist attacks and assumes that served as effective models for Saudi Arabia's policymakers. The first hypothesis is that Saudi Arabia most likely implemented strict criminal law enforcement that includes safeguarding the homeland and

5 Rohan Gunaratna, "Global Terrorism in 2016," UNISCI Journal 40 (January 2016): 135, https://www.ucm.es/data/cont/media/www/pag-78913/UNISCIDP40-8RohanGunaratna.pdf.

6 Ibid., 135.

surveilling borders and residential territories to prevent terrorist attacks. The United States, for example, after the events of September 11, 2001, passed strict laws that include the Aviation and Transportation Security Act that conducted background checks and screening of travelers and their luggage, as well as mandated increased border patrol measures.[7] The laws also implemented a national security strategy that includes detection and identification of terrorist activities and immediate response to prevent any terrorist attack within the United States. Such provisions authorize security forces to detain and investigate any individual suspected to have connection with terrorist organizations.[8]

Similarly, the United Kingdom's Terrorism Act 2000 provided the police the right to arrest suspected individuals and investigate them "without a warrant based on a reasonable suspicion that they have been involved in the preparation, instigation, or commission of acts of terrorism."[9] Laws aimed at protecting the population from terrorist attacks, though, often raised other legal challenges. Statistical records show that "Asian and black people are respectively four and five times more likely to be stopped than white people under this Act."[10] Such measures presented the government of the United Kingdom with the difficult task of protecting individuals' rights while implementing the terrorism act.[11] Thus, Saudi Arabia might have faced the same difficulties of preserving human rights and maintaining strict security measures.

The second hypothesis is that Saudi Arabia also most likely implemented strict cybersecurity measures to track terrorist communications and foil their

---

7 Joshua D. Zelman, "Recent Developments in International Law: Anti-Terrorism-Part One: An Overview," *Journal of Transnational Law and Policy*, 1st ser., 11 (Fall 2001): 4, http://law-wss-01.law.fsu.edu/journals/transnational/vol11_1/zelman.pdf.

8 Ibid., 6, 8.

9 Clare Feikert and Charles Doyle, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States* (CRS Report No. RL33726) (Washington, DC: Congressional Research Service, September 7, 2006), 1,2, https://www.fas.org/sgp/crs/intel/RL33726.pdf.

10 Ibid., 3.

11 Feikert and Doyle, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States*"5.

plans. The United States, for instance, after September 11, 2001, imposed a strict National Cybersecurity Protection System, the National Cybersecurity Protection Plan (NCPP) that works "collaboratively with public, private, and international entities to protect infrastructure, enhance situational awareness and implement analysis, warning and risk-management programs."[12] Such a system effectively blocks all malicious attempts to access "federal executive branch civilian agencies while working closely with those agencies to bolster their defensive capabilities."[13]

The United Kingdom, on the other hand, imposed a variety of methods "supported by the National Cyber Security Program (NCSP), with dedicated funding of £860 million."[14] Such a program supports "a wide range of projects to develop cyber security capabilities and stimulate the UK's cyber security market."[15] For instance, the government has launched a campaign that raises the awareness among businesses "of the threat from cybercrime and espionage and encourages firms to embed effective cyber security risk management practices."[16] While the NCSP protects businesses and organizations, the Defense Cyber Protection Partnership (DCPP) has been initiated "to improve cyber security within the defense supply chain, and continues to focus on best practice, awareness, and proportionate standards."[17]

The third hypothesis is that Saudi Arabia most likely implemented strict banking laws to prevent terrorist fundraising to finance the Islamic State's operation. The United States, for instance, after September 11, 2001, imposed

---

12 U.S. Department of Homeland Security, "Safeguarding and Securing Cyberspace,", January 19, 2016, https://www.dhs.gov/safeguarding-and-securing-cyberspace.

13 Ibid.

14 The United Kingdom, Cabinet Office, *The UK Cyber Security Strategy*, *Report on Progress and Forward Plans*, December 2014, 2, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

15 Ibid.

16 Ibid., 3.

17 Ibid., 15.

strict laws on banks and financial institutions. These laws prohibited "the maintenance of correspondent accounts for foreign banks that have no physical presence in any country."[18] Furthermore, the banks and financial institutions were required to report suspicious activities and to disclose records of the financial institution that were "under investigation for financial crimes related to terrorism."[19] To maintain rigorous counterintelligence investigation, these institutions were required to disclose confidential communications, transaction records, financial reports, and credit information.[20]

## C. SIGNIFICANCE OF THE RESEARCH QUESTION

The contribution of this study is two-fold: its stringent examination of the methods introduced by other nations to successfully respond to and prevent terrorist attacks and the recommendation of appropriate counterterrorism measures that Saudi Arabia can implement to defeat the Islamic State. Since the announcement of the Caliphate, the Islamic State has been striving to expand its influence in the Kingdom of Saudi Arabia, which is a target of utmost strategic interest for the Caliphate. Such interest is reflected in the Islamic State's reference to Saudi Arabia as Wilayat al Haramayn, which means the Province of the Two Holy Places, referring to the Islamic holy sites of Mecca and Medina that are located in the Kingdom.[21] Occupying Mecca and Medina represents an opportunity for the Islamic State to gain legitimacy.

Similarly, Afghanistan has been a target of several global *Jihadi* organizations that believe in the Islamic traditions "about Khorasan (a province in present-day Afghanistan) being the birthplace of an Islamic army that would help

18 Zelman, "Recent Developments in International Law," 5.

19 Ibid.

20 Ibid., 4.

21 Rohan Gunaratna, "Global Terrorism in 2016," 135.

Mehdi establish his Caliphate at Mecca."[22] As a home country for Pakistani Taliban and other militants who have sparked violence in Baluchistan, Karachi, and Waziristan, Pakistan has provided fertile soil for many extremist organizations, "some of which may have ideological affinity with ISIS."[23] Likewise, India has been witnessing militant violence in the Muslim-majority state of Kashmir. Investing in an environment unfriendly to Muslims is another facet of the terrorist agenda; specifically, Abu Bakr al-Baghdadi mentioned India as one of the countries where Muslims' "rights were denied."[24]

The Islamic State continues to expand in this region and to invest in such an ideological environment within the region. The situation and the search for legitimacy provide the Islamic State promising incentives to propose expanding into Saudi Arabia. To foil the Islamic State's plans for legitimacy, Saudi Arabia must implement more comprehensive and multidimensional counterterrorism weapons than the typical mechanized ones. Such sophisticated methods respond to the questions examined by this thesis: what are the legal, financial, and informational counterterrorism measures that Saudi Arabia uses today to respond to Islamic State threats? What additional counterterrorism measures does Saudi Arabia need to implement to combat the Islamic State's threats going forward? What else does Saudi Arabia need to do to foil the Islamic State's plans?

## D. RESEARCH DESIGN

The basic analytic approach of the thesis is a single case study of the counterterrorism measures (legal, financial, and informational) that Saudi Arabia has implemented from 2014 to 2016 to respond to the Islamic State's attacks. First, this thesis explores open source materials to examine how Saudi Arabia

22 Kashif Mumtaz, "ISIS: Assessment of Threat for Afghanistan, Pakistan and South and Central Asia," *Institute of Strategic Studies Islamabad* 36, no. 1 (Spring 2016): 5, http://issi.org.pk/wp-content/uploads/2016/07/1-kashfi_mumtaz_SS_Vol_36_No.1_2016.pdf

23 Ibid., 7.

24 Ibid., 9, 10.

has been responding to the Islamic State's attacks on Saudi soil. Second, it categorizes Saudi Arabia's counterterrorism responses according to legal, financial, and informational measures. Third, the thesis looks at the objectives of Saudi Arabia's use of such measures and the nature of their utilization. This study also presents a detailed analysis of the Islamic State's attacks on Saudi Arabia and the timing of these attacks, offering an inductive explanation of the attackers' motivations. This analysis then helps in testing the three hypotheses presented earlier and in assessing policy implications that lead to recommendations for policymakers focused on new approaches to address the issue of the Islamic State's threats.

## E. THESIS OVERVIEW AND CHAPTER OUTLINE

Chapter II presents a literature review about the Islamic State's military capabilities and provides an overview on the typology of the group's manpower. This overview is based on a review of the scholarly literature on the terrorist group's recruits and methods of recruitment. The literature review also establishes a theoretical framework for analyzing, describing, and testing the previously proposed hypotheses concerning Saudi Arabia's possible measures and responses. The chapter presents a brief review of the Islamic State's cyber capabilities and utilization of such resources. Finally, Chapter II also presents the Islamic State's fundraising capabilities and gives examples of its finance generation methods.

Chapter III provides a brief analysis of Saudi Arabia's counterterrorism responses in accordance with the theoretical framework derived from the literature review analyzing and describing effective counterterrorism measures. This chapter explains Saudi Arabia's criminal law and the use of such law to fight the Islamic State. In this regard, the chapter introduces examples of Saudi Arabia's activation of criminal law enforcement in response to the Islamic State's threats. Additionally, the chapter explains Saudi Arabia's banking laws and regulation to track terrorists' illicit financial resources and the Kingdom's efforts to

tailor its corresponding countermeasures. The chapter also highlights the types of cybersecurity laws and examples their utilization in Saudi Arabia's response to the Islamic State's threats.

Chapter IV provides a brief explanation of Saudi Arabia's counterterrorism responses in accordance with the theoretical framework derived from the literature review analyzing and describing the appropriate counterterrorism measures. To this end, the chapter revisits the fundamental questions of the study and attempts to test the hypotheses against the examples of Saudi Arabia's activation of the comprehensive and multidimensional counterterrorism measures discussed in the previous chapter.

Chapter V concludes the study by evaluating the evidence tested against the hypotheses. This is to examine whether each hypothesis is congruent with the evidence or non-congruent. The chapter also considers policy implications that lead to recommendations for policymakers focused on new approaches to address the Islamic State's threats. Furthermore, the chapter encourages terrorism experts to observe the changing nature of the Islamic State's threats, including the instruments, methodologies, ideologies, targets, sponsorships, and diplomatic strategies employed. Finally, the chapter presents concluding remarks and summarizes the findings of the study.

# II. LITERATURE REVIEW

To assess Saudi Arabia's options to tailor effective, multidimensional responses to the Islamic State's threats, it is essential to begin by reviewing current scholarly literature on that group's military, cyber, and financial resources. This review provides a theoretical framework for analyzing, describing, and testing the hypotheses presented in Chapter I. In particular, the framework derived from the literature review is an aid to examining Saudi Arabia's options for countermeasures addressing the Islamic State's military, cyber, and financial resources.

## A. THE ISLAMIC STATE'S MILITARY CAPABILITIES

As Harleen Gambhir argues, the Islamic state boasts robust manpower that makes the organization capable of "executing a coherent global strategy across its Interior, Near Abroad, and Far Abroad rings."[25] Such parallel efforts grant the organization the resiliency to exert multiple pressures on its adversaries from different directions.[26] The ability to act in multiple locations simultaneously grants the terrorist group an asymmetric advantage over its adversaries.[27] Gabi Siboni, on the other hand, asserts that "the Islamic State is organized along district lines."[28] Each district operates relatively autonomously as do the military forces operating within each district. The organization of these forces is established "in a way that grants them maximal flexibility, with a notable absence

25 Harleen Gambhir, *Middle East Security: ISIS Global Strategy: A Wargame*, Middle East Security Report No. 28, Institute for the Study of War, July 2015, 28, http://understandingwar.org/sites/default/files/ISIS%20Global%20Strategy%20--%20A%20Wargame%20FINAL.pdf.

26 Ibid.

27 Ibid.

28 Gabi Siboni, "The Military Power of the Islamic State," INSS The Institute for National Security Studies, October 8, 2016, 68, http://www.inss.org.il/index.aspx?id=4538&articleid=11166.

of rigid, fixed frameworks."[29] Such looseness enables them to choose "the doctrine, which requires mobility and rapid reinforcement."[30]

According to Siboni, "fighters are recruited from many places, with most coming from the local population in Syria and Iraq."[31] Soon after the Islamic State's announcement of the Caliphate on November 13, 2014, it gained the allegiance of several extremist groups in the Middle East and North Africa, as Rivka Azoulay recounts:

> The Islamic State (IS) Caliph al-Baghdadi issued a rare audio message, 'Even if the disbelievers hate it', in which he acknowledged for the first time that a number of groups in the Middle East and North Africa had pledged their allegiance to IS. The statement followed a series of audio pledges of allegiance three days earlier by groups of mujahedeen in Libya, Yemen and Saudi Arabia, as well as by Jund al-Khilafah (Algeria) and Ansar Bayt al-Maqdis (Sinai Peninsula). The timing and rapid confirmation of these pledges by al-Baghdadi make it likely that they were well prepared in advance. They also reveal a clear IS strategy for expansion beyond Syria and Iraq.[32]

In a short time, the group had control of the areas it captured and it expanded rapidly, equipped with modern weapons and vehicles. Following this rapid beginning, new territories have been announced outside the Middle East, West, and North Africa, such as the Khorasan state in Pakistan.[33] Besides local recruits, the Islamic State has received foreign terrorist fighters, around 36,500 fighters from more than 100 countries since 2012, among them more than 6,600 Westerners from Europe and North America.[34] The organization has

---

29 Siboni, "The Military Power of the Islamic State," 68.

30 Ibid.

31 Ibid.

32 Rivka Azoulay, *Islamic State Franchising Tribes, Transnational Jihadi Networks and Generational Shifts*, CRU Report, April 2015, 10, http://www.clingendael.nl/sites/default/files/Rivka Azoulay_Islamic_State_expansion_CRU_April2015.pdf.

33 Ibid.

34 Christopher M. Blanchard and Carla E. Humud, *The Islamic State and U.S. Policy* (CRS Report No. R43612) (Washington, DC: Congressional Research Service, February 9, 2016), 2, https://fas.org/sgp/crs/mideast/R43612.pdf.

demonstrated extensive military capabilities enabling it to govern and control the captured territories and launch global attacks, which provide a wealth of services to its members.[35] Among this huge number, Saudi fighters represent the largest group of foreign fighters.[36]

The Islamic State capitalizes on the returnee fighters to recruit more fighters and launch deadly attacks on Saudi soil. In India, for instance, the return of Aarif Majeed to India from Iraq in late 2014 marked a turning point in terrorism.[37] Majeed, a young man from the state of Maharashtra, received training from the Islamic State in Iraq to recruit Indians and launch attacks in India.[38] Following his return, in December 2014, Mehdi Masroor Biswas, a Bengaluru-based engineer "was arrested for allegedly managing and running the influential pro-Islamic State Twitter account."[39]

To combat such extensive and flexible capabilities, Saudi Arabia must tailor multidimensional countermeasures. Such methods must enable the Kingdom to confront attacks on Saudi soil and fight against the Islamic State in Iraq and Syria, from which the threats originate. Furthermore, these developed countermeasures must be legally mandated and guided by a coherent policy. Following the September 11, 2001 events, for example, the United States passed and strictly enforced new legislation for safeguarding the homeland and strengthening surveillance of borders and residential territories to prevent terrorist attacks.[40] Similarly, the United Kingdom increased criminal law

35 Blanchard and Humud, *The Islamic State and U.S. Policy*, 4, https://fas.org/sgp/crs/mideast/R43612.pdf.

36 Aaron Y. Zelin, *The Saudi Foreign Fighter Presence in Syria*, Washington Institute Report No. 7, Issue 4, April 2014, 10, https://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20140428-CTCSentinel.pdf.

37 Animesh Roul, "India Faces Up to Growing Islamic State Threat," *Terrorism Monitor* 13, no. 17 (August 21, 2015): 6, https://jamestown.org/wp-content/uploads/2015/08/TerrorismMonitorVol13Issue17_02.pdf.

38 Ibid.

39 Ibid.

40 Feikert and Doyle, *Anti-Terrorism Authority*, 1.

enforcement measures to safeguard its homeland and prevent terrorist offensives.[41] Such measures and their implications are discussed in Chapter III.

## B. THE ISLAMIC STATE'S CYBER CAPABILITIES

A technical analysis group asserts that many Islamic jihad members demonstrate strong technical knowledge and social media skills. They utilize such knowledge for communications, recruitment, training, and surveillance.[42] Furthermore, they use "cyberspace and cyber technology to raise money in a number of ways."[43] Similarly, the Islamic State invests in online strategies demonstrating successful use of social media and cyberspace for propaganda, training, recruitment, and fundraising.[44] Adam Hoffman and Yoram Schweitzer assert that as a basic part of the Islamic State's efforts to publicize its ideology in the Middle East and globally, the organization designs online propaganda materials and disseminates these materials using its English-language magazine known as *Dabiq*.[45] Additionally, the group "produces high quality movies that are disseminated on YouTube, Twitter, and various websites affiliated with the organization."[46]

Like the United States and the United Kingdom, Saudi Arabia must tailor the effective countermeasures to confront the fundraising, propaganda, and recruitment taking place on Saudi soil as well as in cyberspace. After September 11, 2001, the United States imposed strict surveillance law on electronic communications represented in emails, phone calls, and text messages to track

41 Ibid.

42 Technical Analysis Group, *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Institute for Security Technology Studies at Dartmouth College, Technical Analysis Group, November 2003, 19, http://www.ists.dartmouth.edu/library/164.pdf.

43 Ibid.

44 David P. Fidler, *Countering Islamic State Exploitation of the Internet*, Digital and Cyberspace Policy Program Cyber Brief, June 2015, 1, http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-Internet/p36644.

45 Adam Hoffman and Yoram Schweitzer, "Cyber Jihad in the Service of the Islamic State (ISIS)," INSS The Institute for National Security Studies, March 20, 2015, 72, 73, file http://www.inss.org.il/uploadImages/systemFiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf.

46 Ibid.

terrorist activities and to introduce immediate countermeasures.[47] Encryption and its related technologies, which are often employed by terrorists, adopt high privacy and security levels that are described as "presenting hurdles for law enforcement and intelligence officials."[48] Amnesty International defines encryption as:

> Encryption is a technical term used to describe the manner by which communications—text messages, emails, phone calls and video chats—are secured against access by anyone who is not the intended recipient. The act of encryption is the mathematical manipulation of information to render it readable solely by the person or persons intended to receive it. Although encryption existed long before the Internet—one of the earliest forms of encryption was the Caesar Cipher, developed by Julius Caesar to secure the written notes carried by messengers—the advent of digital technologies and the Internet has moved encryption from the sole preserve of cryptographers, to being a concern for every Internet user.[49]

Law enforcement, however, often requires breaking into technological devices and removing encryption for purposes of surveillance. This capability gives investigators a "large amount of information … at their fingertips—access to location data, information about individuals' contacts, and a range of websites—[enabling them to] collectively form 'digital dossiers" on individuals.'[50] Yet, the individual's right to privacy and the inherently secure nature of modern communications technology can make gaining access to personal communication devices increasingly difficult for law enforcement. Technology companies such as Apple and Google have "implemented automatic full-device encryption for mobile devices and automatic encryption for certain

---

47 Feikert and Doyle, *Anti-Terrorism Authority*, 14.

48 Kristin Finklea, Richard M. Thompson II, and Chris Jaikaran, *Court-Ordered Access to Smart Phones: In Brief* .(CRS Report No. R44396) (Washington, DC: Congressional Research Service, February 23, 2016), 1, https://www.fas.org/sgp/crs/misc/R44396.pdf.

49 Amnesty International, *Encryption: A Matter of Human Rights*, March 2016, 6, https://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

50 Ibid.

communications systems."[51] Using such strong encryption, these companies "assert they do not maintain encryption keys and therefore cannot unlock, or decrypt, the devices or communications—not even when presented with a court authorized wiretap order."[52]

Following the terrorist attacks in Paris, France, and San Bernardino, California, in November and December of 2015, "U.S. investigators recovered a cell phone reportedly used by one of the shooters."[53] To support the investigation, on February 16, 2016, the U.S. District Court for the Central District of California ordered Apple, Inc:

> Under the All Writs Act to provide "reasonable technical assistance to assist law enforcement agents in obtaining access to the data" on the cell phone for which the government had already obtained a probable cause warrant. The order directs Apple's assistance to feature three components: bypass or disable the iPhone's auto-erase after 10 incorrect passcode attempts function (even if the function has not been enabled); enable the FBI to electronically input passcodes for testing; and ensure there is no added delay between passcode attempts.[54]

Apple Company opposed the order, which would have required changes to the design and manufacture of their product, believing "if the technology then falls into the wrong hands, it could potentially be exploited by criminals and other malicious actors."[55] The case raised "much debate over whether the government's request in the San Bernardino case would constitute the creation of a so-called 'back door' or 'master key' to the iPhone's encryption."[56] Such an incident represents one of many ways in which terrorists utilize cyber technology not only to recruit members but to orchestrate attacks. Similar to the United States, the United Kingdom adopted a variety of methods at their disposal to

51 Finklea, Thompson, and Jaikaran, *Court-Ordered Access to Smart Phones*, 1.

52 Ibid.

53 Finklea, Thompson, and Jaikaran, *Court-Ordered Access to Smart Phones*, 1.

54 Ibid., 2.

55 Ibid.

56 Ibid.

investigate crimes. Among such methods was the "interception of communications, electronic data, and various forms of surveillance."[57] Introducing such measures in Saudi Arabia would enhance the capabilities of security forces to combat the Islamic State's cyber-attacks on Saudi territories.

## C. THE ISLAMIC STATE'S FUNDRAISING CAPABILITIES

As terrorism experts argue, terrorist organizations despite their structural, operational, motivational, recruitment differences and differences in capabilities, always strive to find critical resources to finance for their long-term survival and launching attacks.[58] Without finance, it is difficult for a terrorist group to build an infrastructure that can foster management capabilities, recruitment, training, salaries, public services, and social welfare capabilities. Therefore, terrorist organizations strive to generate money through the exploitation of natural resources, solicitation of donations, establishment of charitable organizations, and the pursuit of illegal activities.[59]

As Carla E. Humud, Robert Pirog, and Liana Rosen point out, according to media reports and documents captured in the battlefield, the Islamic State generates finance mainly from natural resources revenue, illegal activities, donations, and antiquities.[60] Among these various revenue sources, donations and illegal activities such money laundering represent the most important ones for the Islamic State. The Financial Action Task Force report in 2015 estimated that the Islamic State collected about $360 million from money laundering and bank looting.[61]

---

57 Feikert and Doyle, *Anti-Terrorism Authority*, 13.

58 The Financial Action Task Force, *Emerging Terrorist Financing Risks*, October 2015, 9, 10, www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.

59 The Financial Action Task Force, *Emerging Terrorist Financing Risks*, 10, 11.

60 Carla E. Humud, Robert Pirog, and Liana Rosen, *Islamic State Financing and U.S. Policy Approaches* (CRS Report No, R43980)(Washington, DC: Congressional Research Service, April 10, 2015), 10, https://www.fas.org/sgp/crs/terror/R43980.pdf

61 United States Committee on Financial Services, *Task Force to Investigate Terrorism Financing Hearing Entitled "A Survey of Global Terrorism and Terrorist Financing*, U.S. House of Representatives, April 22, 2015, 5, 6, http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=398891.

Among these different sources of funding, natural resources have been central to the Islamic State's flow of money. Controlling the Syrian oil rich territories, the Islamic State, has benefited significantly in oil revenue. The militants exploit oil to finance and operate its vehicles in the areas controlled by the group.[62] In particular, the group sells or trades crude oil. The product is shipped to the Syrian-Turkish border, where it is exchanged for money or exchanged for necessary supplies.[63] In addition to the Syrian oil fields, the Islamic State also controls several oil rich fields in northern Iraq. Many reports allege that the militants make significant amounts of income from oil transactions that promised attractive prices to potential buyers before world oil prices tumbled:

> ISIS oil might have been selling for as little as $18 per barrel at the Turkish border, when Brent, a world price reference crude oil was selling for about $107 per barrel. Recently, the price of Brent has declined to about $65 per barrel, a decrease of over 50% since June 2014. The fall in world oil prices has likely further reduced the net price received by IS leaders for the oil they sell.[64]

Likewise, the group gains considerable income from foreign fighters and donors in the Gulf and European states, though these amounts do not surpass the money generated from other resources.[65] According to some estimates, the "Islamic State in 2013–14 accumulated up to $40 million from donors in Saudi Arabia, Qatar, and Kuwait."[66] These donors, as Magnus Normark and Magnus Ranstorp argue, utilize a traditional transfer system known as hawala operating in the Islamic State's terrorist networks around world.[67] It is frequently observed that the organizations "financial transactions are conducted through a web of

62 Ibid., 5.

63 Ibid., 5.

64 Humud, Pirog, and Rosen, *Islamic State Financing*, 5.

65 Ibid., 9, 10.

66 Ibid.

67 Magnus Normark and Magnus Ranstorp, *Understanding Terrorist Finance, Modus Operandi and National CTF Regimes*, Report no. 46, December 18, 2015, 19, 20, http://www.fi.se/upload/43_Utredningar/20_Rapporter/2016/Understanding_Terrorist_Finance_160315.pdf

hawaladar underground networks established throughout Iraq, Syria and beyond."[68]

Such an underground money transfer network for funding the Islamic State or other terrorist groups seems quite dangerous for Saudi Arabia. This is because many Saudis may find a way to receive or transfer money to fund terrorist activities on Saudi soil. Like the United States, Saudi Arabia must impose strict laws to prevent the Islamic State's fundraising on Saudi soil. Specifically, the United States, after September 11, 2001, imposed strict laws on banks and financial institutions.[69] The laws enabled security forces to maintain a stringent counterintelligence investigation as these institutions were required to disclose confidential communications, transaction records, financial reports, and credit information.[70] The policy implications of such measures and their implementation for Saudi Arabia's counterterrorism efforts are considered in the following chapter.

68 Ibid.

69 Zelman, "Recent Developments in International Law," 5.

70 Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

## III. SAUDI ARABIA'S COUNTERTERRORISM RESPONSES

After the events of September 11, 2001, Saudi Arabia among other states adopted strict counterterrorism measures as a response to UN Security Council Resolution 1373, which requires all member States to prevent and suppress "the financing of terrorist activities by criminalizing all acts tending to provide for or facilitate such financing."[71] Furthermore, member states are required to refrain from "providing any assistance or support, passive or active, to persons or entities involved in terrorist activities."[72] Additionally, member states are required to enhance "cooperation among themselves through the exchange of information and other measures to control and impede the movement of terrorists across international boundaries."[73] Saudi Arabia, in particular, has imposed strict countermeasures represented in criminal law enforcement, cyber-security laws, and banking laws as detailed in this chapter.[74]

To provide a brief analysis of Saudi Arabia's counterterrorism responses in accordance with the theoretical framework derived from the literature review in Chapter II, which analyzes and describes effective counterterrorism measures by the United States and the United Kingdom, this first section explains how Saudi Arabia has utilized strict criminal law enforcement to fight the threats promoted by the Islamic State. Therefore, the chapter introduces examples of Saudi Arabia's activation of criminal law enforcement in response to the Islamic State's threats. Furthermore, the chapter highlights the types of cybersecurity laws and examples of how Saudi Arabia can use them in response to these threats. And, the final section examines Saudi Arabia's banking laws and regulation to track

71 The Law Library of Congress, "Algeria, Morocco, Saudi Arabia: Response to Terrorism," report, September 2015, 2, https://www.loc.gov/law/help/counterterrorism/response-to-terrorism.pdf.

72 Ibid.

73 Ibid.

74 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," April 4, 2016, 3, https://28pagesdotorg.files.wordpress.com/2016/05/saudi-lobby-white-paper.pdf.

terrorist illicit financial resources and how these laws can be used to tailor effective countermeasures.

## A. CRIMINAL LAW ENFORCEMENT

Besides counterterrorism efforts against al-Qaida, the Kingdom of Saudi Arabia has increasingly focused these efforts, both domestically and internationally, "on the threat posed by the Islamic State in Iraq and the Levant (ISIL), as well as Saudi citizens returning from fighting in Syria."[75] Such multidimensional efforts are explained separately in detail in the following paragraphs.

### 1. Domestic Efforts

The Kingdom of Saudi Arabia has adopted a broad range of security and safety measures for "domestic security and counterterrorism, civil defense, criminal investigations and counterespionage, prison administration, passports and border security, and infrastructure protection."[76] Such tasks are enhanced by new counterterrorism legislation. The legislation criminalizes all acts proven to create a disturbance to public order, damage the image of Saudi Arabia, or threaten its national unity.[77] In reporting to the UN Security Council Committee on its adoption of Resolution 1373 with regard to counterterrorism, Saudi Arabia asserted the *hirabah* Act derived from Shariah Law as follows:

> In the Islamic Shariah, which the Kingdom applies and from which it derives its statutes, crimes of terrorism are included among the crimes of hirabah. The severest of penalties are applied to these crimes in the Islamic Shariah, as set forth in the Holy Koran [Koran 5:33]. The crimes of hirabah include the killing and terrorization of

75 United States Department of State Bureau of Counterterrorism, *Country Reports on Terrorism 2014*, June 2015, 208, accessed January 23, 2017, https://www.state.gov/documents/organization/239631.pdf

76 Boucek, "*Saudi Arabia's "Soft" Counter-terrorism Strategy*" 5.

77 The Law Library of Congress, "Algeria, Morocco, Saudi Arabia: Response to Terrorism," 2.

> innocent people, spreading evil on earth (al-ifsad fi al-ard), theft, looting and highway robbery.[78]

To achieve security and stability all over the Kingdom, combat all types of crimes, ensure the safety of all Saudi people and Pilgrims, the new law grants the Minister of Interior the power to "reinforce security relationships with neighboring Arab countries, as well as the broader Arab world."[79] This is "to maintain safety in the Kingdom and abroad, control crime, fight terrorism and drug smuggling, exchange security information."[80] Such a relationship is meant to "organize citizenship regulations and systems, and develop Arab security institutions."[81] The new law empowers the Minister of Interior to authorize security forces to "enter homes and offices at any time for the purpose of searching them and arresting persons accused of terrorist crimes."[82]

By this, the ministry then possesses jurisdiction over many sectors, such as the public security sector for traffic control and police, as well as the premises security sector, which protects "government buildings and facilities, as well as manning check points."[83] Such jurisdiction is in addition to civil defense and Special Forces, which carries out "special and emergency security operations."[84] The Saudi General Investigations Directorate, on the other hand, conducts counterterrorism investigations and transfers cases "to the Special Investigations and Public Prosecutions Office in the Saudi Ministry of Justice for the duration of the trial."[85]

---

78 Ibid., 5.

79 Hamza A. Baitalmal, "Conceptual Framework of Saudi Arabia's Efforts in Countering Terrorism: The Case of Intellectuals and Mass Media," Harvard University, 2016, 8, http://scholar.harvard.edu/majidrafizadeh/BaitalmalSAEfforts.

80 Ibid., 8, 9.

81 Ibid., 9

82 The Law Library of Congress, "Algeria, Morocco, Saudi Arabia: Response to Terrorism,"6.

83 Baitalmal, "Conceptual Framework of Saudi Arabia's Efforts in Countering Terrorism," 9.

84 Ibid.

85 United States Department of State Bureau of Counterterrorism, *Country Reports on Terrorism 2014*, 209.

The Saudi authority has also established a "Specialized Criminal Court" controlled by the judicial authority to undertake trials of detained individuals involved in or accused of, terrorist crimes, as well as cases related to state security.[86] This Specialized Criminal Court held its first hearings in June of 2011 considering the case of 85 persons who were accused of being connected "to Al-Qaeda, and participating in the bombings of several housing compounds in Riyadh, in 2003."[87]

Being granted such broader power, in May 2014, the Saudi Ministry of Interior tracked an estimated 1,200 Saudi citizens who had gone to join the war in Syria, with some other sources estimating the number at 2,500 Saudi nationals or even more.[88] Thus, in September of 2015, Saudi security forces arrested 1,300 Saudis and approximately 300 foreign nationals alleged to be associated with Daesh/ISIL "organization, reflecting the government's firm approach to perceived domestic security threats."[89] To deal with such situations, the Saudi authorities have imposed tougher prison sentences ranging from three to 20 years for Saudis who travel abroad to join in fighting with a terrorist organization.90

### 2. International Efforts

In addition to domestic counterterrorism measures, the Kingdom has increased its international efforts by participating "in international counterterrorism conferences and engagements."[91] For instance, Saudi Arabia has maintained a strong counterterrorism relationship with the United States to ensure the security of "both United States and Saudi citizens within Saudi

86 Baitalmal, "Conceptual Framework of Saudi Arabia's Efforts in Countering Terrorism," 8.

87 Ibid.

88 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism,"41.

89 Ibid., 47.

90 Ibid., 41.

91 Ibid., 208.

territories and abroad."[92] Additionally, Saudi Arabia has joined the Global Coalition to Counter ISIL, supporting coalition efforts with military action. The United States Department of State Bureau of Counterterrorism, in its Country Reports on Terrorism in 2014 asserts:

> Its external actions against ISIL was complemented by an aggressive campaign by both official clerics and Saudi King Abdullah to discredit the group and condemn their activities as acts of terrorism. The Kingdom of Saudi Arabia welcomed UN Security Council Resolutions 2170 and 2178, expanding existing counterterrorism programs and rhetoric to address the phenomenon of foreign terrorist fighters, and leveraged terrorist finance provisions of its Law for Crimes of Terrorism and Terrorist-Financing (CT Law) to combat funding of violent extremist groups in Iraq and Syria.[93]

The Kingdom of Saudi Arabia has fully participated in all regional and international counterterrorism initiatives, "including by participating in the Global Counterterrorism Forum."[94] Notably, Saudi Arabia hosted the Muslim World League, which was attended by 500 Muslim scholars in Makkah in June 2008. Furthermore, Saudi Arabia fully participated in the second conference held in Madrid, Spain, in July 2008, which was attended by "300 delegates of different faiths such as Islam, Buddhism, Christianity, Hinduism, and Judaism."[95] In November of the same year, Saudi Arabia joined the UN General Assembly on Interfaith Dialogue.[96] More recently, Saudi Arabia joined the Camp David Summit in May 2015, when the Kingdom with five other Gulf nations issued a joint statement on the Task Force on Counterterrorism and Border Security of the U.S.-Gulf Cooperation Council Strategic Cooperation Forum (SCF), founded in March 2012.[97]

---

92 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 208.

93 Ibid.

94 United States Department of State Bureau of Counterterrorism, *Country Reports on Terrorism 2014*, 210.

95 28pages.org," The Kingdom of Saudi Arabia and Counter-Terrorism," 39.

96 Ibid.

97 28pages.org,"The Kingdom of Saudi Arabia and Counter-Terrorism," 15.

## B. SOFT COUNTERTERRORISM MEASURES

Besides strengthened laws and stricter law enforcement, the Kingdom has adopted soft counterterrorism measures represented in its prevention, rehabilitation, and aftercare programs.[98] These programs aim to deter Saudis from involvement in radicalization, offer rehabilitation counseling and means, and provide aftercare programs to individuals involved in radicalization to "facilitate [their] reintegration into society after their release from custody."[99] It is worth explaining each program separately in detail in the following paragraphs.

### 1. Prevention

The Kingdom of Saudi Arabia has established many programs run by the government aimed at prevention of radicalization and extremism. Such programs include education of the "public about radical Islam and the dangers of extremism, as well as programs designed to short-circuit radicalization by providing alternatives."[100] The Guidance Department at the Ministry of Interior has played a vital role in the implementation of many such programs which "are designed to confront extremism through the promotion and propagation of a more judicious interpretation of religious doctrine—absent takfir."[101] The believers of the takfir doctrine, as asserted by scholars, tend to accuse other Muslims of "being an apostate—and are focused on strict jurisprudence of recognized scholars and authorities."[102]

The main concern of the Kingdom is not the audience of the extremists themselves, rather it is the "larger population that may sympathize with extremists and those who do not condemn the beliefs that lead to extremism."[103]

---

98 Boucek," Saudi Arabia's "Soft" Counter-terrorism Strategy," 4.

99 Ibid.

100 Ibid., 8.

101 Boucek," Saudi Arabia's "Soft" Counter-terrorism Strategy,"8.

102 Ibid.

103 Ibid.

The strategy of prevention focuses on combating radicalization "by monitoring radical websites and by promoting more moderate views through education, media, and entertainment."[104] To achieve such goals and prevent radicalization and recruitment of young men, the prevention program has created many activities that keep young men "busy and away from radicals."[105] These activities include sport events, car and camel racing, and summer camping where scholars give lectures that condemn extremism. Additionally, the Ministry of Culture and Information "has initiated a series of projects—some for youths and some for adults—utilizing television, newspapers, and other forms of communication."[106] In the province of Asir, for instance, working with the Ministries of Education and Culture and Information and the local media, the regional government produced a book about Asir province's achievements so far "to raise awareness for the dangers posed by extremism and radicalization."[107]

These projects employ scholars and religious figures who speak about extremism and its danger to Islam and Muslims. The Ministry of Islamic Affairs, on the other hand, sponsors religious "lectures and classes at mosques throughout the country, utilizing speakers and materials recommended by experts on extremism."[108] At schools throughout the Kingdom, the Ministry of Education gives lectures and classes to raise the awareness of the "students from a very early age about the dangers of extremism and the effects of terrorism and violence."[109] Similarly, in public streets and main roads, Saudi authorities post billboards, images, and photos of terrorists' attacks to raise public awareness about the danger of terrorism.[110]

---

104 Gabriel Hoeft, "'Soft' Approaches to Counter-Terrorism: An Exploration of the Benefits of Deradicalization Programs," The International Institute for Counter-Terrorism (ICT), Spring 2015, 31, https://www.ict.org.il/UserFiles/ICT-Soft-Approaches-to-CT-Hoeft.pdf.

105 Boucek," Saudi Arabia's "Soft" Counter-terrorism Strategy," 8.

106 Ibid.

107 Boucek," Saudi Arabia's "Soft" Counter-terrorism Strategy," 9, 10.

108 Ibid., 8.

109 Ibid.

110 Ibid., 10.

### 2. Rehabilitation

The Kingdom of Saudi Arabia runs a rehabilitation process, under the Counseling Program, which is administered by the Ministry of Interior. The process is overseen by an Advisory Committee consisting of four subcommittees: The Religious Subcommittee; the Psychological and Social Subcommittee; the Security Subcommittee; and the Media Subcommittee.[111] The Advisory Committee visits all jails in Saudi Arabia to meet with detainees across the state and refers their cases to the appropriate subcommittees. The Religious Subcommittee, for instance, includes clerics, scholars and university professors who "directly engage in the prisoner dialogues and the counseling process."[112] The Psychological and Social Subcommittee, which consists of psychologists, psychiatrists, social scientists, and researchers, on the other hand, evaluates the prisoners' social and psychological backgrounds related to their cases.[113]

Once the process of assessment and counseling concludes, the detainees are referred to the "Security Subcommittee [whose role] is to evaluate prisoners for security risks."[114] Based on its assessment and the input of the Religious Subcommittee and the Psychological and Social Subcommittee, the Security Subcommittee issues release recommendations.[115] Additionally, the Security Subcommittee advises the detainees in terms of behavior upon release and future direction.[116] Detainees are always made aware that they will be monitored regularly wherever they live. Similar to the efforts of other subcommittees, the Media Subcommittee produces Internet, radio, televised, and printed

111 Christopher Boucek, "Counter-Terrorism from Within Assessing Saudi Arabia's Religious Rehabilitation and Disengagement Programme," RUSI 135, no. 6 (December 19, 2008): 61, http://carnegieendowment.org/files/boucek_rusi.pdf.

112 Boucek, "Counter-Terrorism from Within," 61.

113 Hoeft, "'Soft' Approaches to Counter-Terrorism," 35.

114 Boucek, "Counter-Terrorism from Within," 61.

115 Ibid., 62.

116 Ibid.

"educational materials for use in prevention programs in schools and mosques."[117]

In terms of the effectiveness of rehabilitation, Saudi government reports show that the program has achieved "a success rate of 80–90 percent."[118] The remaining 10 to 20 percent are either non-participants or "those who reoffended upon release."[119] In other words, "only 35 of the 1,400 prisoners who completed the program and were released had been rearrested."[120] A stark example of its failure, though, was the return of at least 11 Saudi detainees from Guantanamo Bay to their terrorist organizations, as the U.S. Department of State report asserts.[121]

### 3. Aftercare Programs

Aftercare programs are pre-release programs run by the Religious Subcommittee targeting the "detainees who have completed their prison sentences and are assessed as suitable for release."[122] These detainees are transferred to a halfway house program where they live for some months to prepare for reintegration into society and wash away their radical ideologies.[123] Once the detainees have changed their radical mindset, they are provided

117 Ibid.

118 Hoeft, "'Soft' Approaches to Counter-Terrorism," 36.

119 Ibid.

120 Ibid.

121 Hoeft, "'Soft' Approaches to Counter-Terrorism," 36.

122 Abdulrahaman Al-Hadlaq, "Terrorist Rehabilitation: The Saudi Experience," in *Terrorist Rehabilitation and Counter-Radicalization: New Approaches to Counter-Terrorism* (New York: Routledge, 2011), 65, https://books.google.com/books?id=1fWrAgAAQBAJ&pg=PA68&lpg=PA68&dq=CounterTerrorism+from+Within:+Assessing+Saudi+Arabia%27s+Religious+Rehabilitation+and+Disengagement+Programme+pdf&source=bl&ots=JwHaXUDhiU&sig=caTkZeg0M4kruSMEHBKUtfUUTM&hl=en&sa=X&ved=0ahUKEwiTvsz579HRAhUlqFQKHZ62A80Q6AEIITAB#v=onepage&q=Counter-Terrorism%20from%20Within%3A%20Assessing%20Saudi%20Arabia's%20Religious%20Rehabilitation%20and%20Disengagement%20Programme%20pdf&f=false

123 Ibid., 66.

financial support, jobs, apartments, cars, and many other benefits. Detainees who were previously government employees are assisted back to their jobs.[124]

Additionally, rehabilitated individuals are provided with materials such as "books and audio-visual material propagating moderate Islam."[125] Such programs have yielded great success in deterring radicalization; nonetheless, Saudi authorities have faced some challenges related to the high cost and necessary cooperation for the program.[126] In particular, program administrators must enlist graduates of the rehabilitation program to share their success stories. Saudi officials, for instance, have repeatedly reported that prisoners who have already been deradicalized reflect and "share their experiences in media campaigns."[127] Such reflected experience, as reported by officials, contributes significantly "to prevent future radicalization among key demographics."[128]

Additionally, stories narrated by deradicalized individuals have a great impact on changing the mindset of current detainees who "sympathize with the prisoners' experiences."[129] The key reason the Saudi program has been so successful is that the government has invested tremendous resources in providing a unique approach that is individually tailored to each prisoner, including ongoing counseling, financial support, and career development assistance after graduation from the program.[130]

Ben Emmerson, the United Nations special rapporteur on counterterrorism and human rights, praised the Saudi counterterrorism soft measures, saying, "I

---

124 Ibid., 67.

125 Ibid.

126 Al-Hadlaq, "Terrorist Rehabilitation: The Saudi Experience," 67.

127 Johann Carlos Barcena, Kenneth Daines, and John Noh, *Combatting Terrorism Through Prosecutions & Rehabilitation: Three Models Compared*, A Report to the Bureau of Conflict & Stabilization Operations U.S. Department of State, Stanford Law School, June 2015, 27, https://law.stanford.edu/publications/combating-terrorism-through-prosecutions-rehabilitation-three-models-compared-a-report-to-the-bureau-of-conflict-stabilization-operations-u-s-department-of-state/.

128 Ibid.

129 Ibid.

130 Ibid., 25.

can confidently say that the Mohammed bin Naif Counseling and Care Center is a high example to be followed."[131] Press statements, such as thje following one from al-Arabiya, echo his assessment:

> Emmerson said he was personally acquainted with the situation of the detainees and those accused of terrorism charges in Al-Hair Prison, and can vouchsafe that the general situation in sections and wings of the public security prison in Al-Hair, Riyadh, takes into account the human rights of the detainees in general, starting from cells exposed to sun and air to health care, and the prison is run at extremely high levels. He also praised a package of measures followed by the Saudi authorities, including follow-up of families whose sons were involved in terror acts, support given to terror victims, or allowing those accused of terrorism to have continuous contact with their families, whether they are Saudis or residents. He said the Mohammed bin Naif Counseling and Care Center is considered a unique center for adopting programs based on an integrated process that combines social and psychological treatment, as well as economic support such as provision of jobs to the beneficiaries of the program. The center is also unique in providing other activities such as treatment through painting, religious follow-up for those carrying ideas deviant to the proper Islamic teachings, to have them integrated into the community as effective members through programs and activities adopted by the center.[132]

### C. CYBERSECURITY LAWS

According to the Communications and Information Technology Commission in Saudi Arabia annual report, 2013, the number of Internet users in the Kingdom of Saudi Arabia has increased rapidly, as have cyber-crimes across the Saudi state. For instance, cyber-attacks, such as that against Aramco Oil

---

131 Mohammed Bin Naif Counseling and Care Center, Media Center, "UN Rights Official Commends Saudi Prison Conditions," news release, April 19, 2017, Mohammed Bin Naif Counseling and Care Center, https://www.moi.gov.sa/wps/portal/!ut/p/z1/rVNLU8IwEL7zK-qBYyePpq9jYRAEtdiK0Fw6MWQgDk15VNB_bzqMM0KFwugeNq9vH_l2F9CGYTQaYKIXvfmpDg6AKraVM1bIXLEFmICEOim8I6SHCB5AYnVgYLut56dhH8E2AeMjgB21YeA4oy5xIkjuEaAX2Z-QAF5o_w0IB6GrAa3H_q0_RDC0r7Q_Alj23-J3a-1fAAWUq2JZzEGSMamakOfvaiMWUs0MLlQh1k24f1Bit9lrg635XG6FfuGcp-VVij0TIRND5LBUqNLtkspSIQnIOFTZrrM903i-7bJbIZNC3H8yrGDLcxraNB50vNV6h_-s1qGcZlQDdNnfXQrgF96rS7N8yECG8SauURz4Z5KNHQQGG-l2IGRyteZHpH4Sqp7FbaqbOuxk2-rFQ10b-S6BT4KMPnP5lhmo1Iyz_o046gTeQ8di9Dk5gsshTBj/dz/d5/L2dBISEvZ0FBIS9nQSEh/.

132 Ibid.

Company and the King Saud University website in August 2012, have raised Saudi Arabia's information security awareness.[133] This awareness is particularly heightened considering that the Kingdom's losses from cyber-attacks reached SR 2.6 billion in 2012 alone.[134] Although Mike Lennon deems the Islamic State's cyber capabilities limited now, he warns "this is something that can change rapidly. Launching damaging cyberattacks does not require a large team, and by recruiting or training a group with a higher level of skill, the threat should not be brushed off."[135]

Reports on Saudi Arabia' cyber-security and information warfare highlight the Kingdom's efforts to achieve superiority in this area:

> In February 2013, the International Data Corporation (IDC) reported that Saudi Arabia invested the most of any country in the Middle East in technology, including cyber capabilities, underscoring the growing importance with which the Kingdom sees cyber-security. The Saudi government and Ministry of Defense have expressed a desire to form a unified department, working in both the public and private sector, specifically tasked to defend the Kingdom against cyber threats.[136]

Beyond its investment in this area, the Kingdom of Saudi Arabia has approved the Anti-cyber-crime Law, which addresses electronic crimes such as "credit card fraud, Internet crimes, cyber terrorism, creation and/or distribution of viruses, hacking, system interference, illegal access and interception."[137] Violators have faced heavy penalties ranging from imprisonment and fine.

---

133 Elnaim, "Cyber Crime in Kingdom of Saudi Arabia," 16

134 Ibid.

135 Mike Lennon, "ISIS Cyber Capabilities Weak, Poorly Organized: Report," Security Week, April 28, 2017, http://www.securityweek.com/isis-cyber-capabilities-weak-poorly-organized-report

136 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 8.

137 Elnaim, "Cyber Crime in Kingdom of Saudi Arabia," 16.

### 1. Combating Terrorists' Cyber-Sabotage

Sabotage cyber-attacks that threaten Saudi Arabia are represented in hacking, virus dissemination, and denial of service attacks. While hackers may access computers to view, copy, or enter data without doing malicious harm, virus disseminators purposely corrupt computer data to cause economic damage.[138] Denial of service attackers, on the other hand, render "computers or network resources inaccessible to their intended users or customers."[139] Such cyber-sabotage on Saudi Arabia has happened frequently, including the latest destructive attack of November 2016 "associated with the 2012 Shamoon attack campaign."[140] It is assumed that the attackers may have "obtained the credentials through a previous, separate attack."[141] This is because "the hardcoded account credentials met Windows password complexity requirements."[142] Robert Falcone explains:

> There were 16 account credentials found hardcoded within the Disttrack payload, appearing to be a mixture of individual user accounts and broader administrator accounts. All but one of the passwords met Windows complexity requirements, specifically, containing uppercase and lowercase characters, and either a number, symbol, or both. One of the general administrator accounts seen in this payload was also in the Disttrack payload in the first Shamoon 2 attack from November 17, 2016, which may not be specific to the targeted organization and instead used as an attempt to guess the login credentials. Based upon the existence of these credentials, it is highly likely the threat actors had carried out a previous attack to obtain these account credentials, as it is unlikely that these passwords were guessed or brute forced.[143]

---

138 Elnaim, "Cyber Crime in Kingdom of Saudi Arabia," 14.

139 Ibid., 15

140 Robert Falcone, "Second Wave of Shamoon 2 Attacks Identified," Paloalto Network, January 9, 2017, http://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/?__hstc=67007217.dfbe03a820b4634fff1f3b6349592f70.1484912948051.1484912948051.1484912948051.1&__hssc=67007217.1.1484912948053&__hsfp=3179728420.

141 Falcone, "Second Wave of Shamoon 2 Attacks Identified."

142 Ibid.

143 Falcone, "Second Wave of Shamoon 2 Attacks Identified."

By attacking such a large number of government websites, especially oil companies, attackers intended to cause the Saudi state as much financial damage as they could. This is because the time consumed and the money spent to fix these sites come at the burden of Saudi government.[144] Although it was not officially confirmed that these attacks were conducted by the Islamic State, the Islamic State's cyber-attacks against Saudi Arabia are reflected in the attack launched by the group known as the Cyber Caliphate.[145] From Birmingham in England, the jihadist Junaid Hussain set up the group and urged his followers to hack more than 54,000 Twitter accounts belonging to users in Saudi Arabia.[146] The hackers, after hijacking the accounts, "leaked online personal information of the victims, including phone numbers and passwords, exposing them to serious risks."[147]

### 2. Combating Terrorists' Exploitation of Social Media to Commit Cyber-Crimes

Cyber-crimes for propaganda are usually related to the Islamic State, which heavily invests in social media for recruiting and training members to carry out attacks on Saudi soil. For instance, just recently in Hail province north of Saudi Arabia, two brothers killed their relative horrifically, filmed the scene of the execution, and "promptly posted the video online using a mobile device."[148] Additionally, they disseminated the video to other social media such as Twitter in support of the Islamic State's propaganda.[149]

---

144 Ibid.

145 Pierluigi Paganini, "Cyber Caliphate Hacks 54k Twitter Accounts, including Ones of CIA and FBI Officials," *Covai Post*, November 15, 2015, section goes here, http://www.covaipost.com/aroundtheweb/cyber-caliphate-hacks-54k-twitter-accounts-including-ones-of-cia-and-fbi-officials/.

146 Ibid.

147 Ibid.

148 Michael S. Smith II, "Social Media Jihad" (speech, NC-SC Counterterrorism Conference, National Sheriff's Association, North Charleston, South Carolina, February 15, 2016), http://kronosadvisory.com/NC.SC.CT.Conf.SocialMediaJihadPresentationRemarks.pdf.

149 Ibid.

To counter such threats, Saudi Arabia imposed strict laws against computer based cyber-crimes by prescribing heavy penalties for hacking into websites, assisting terrorist individuals or groups in the design or operation of a website, or using a website to disseminate information or instructions on related to making explosive devices.[150] Furthermore, the Kingdom has launched a media campaign that includes the Saudi Council of Senior Ulama and other senior religious scholars' condemnations of terrorism, via television interviews, shows, and "advertisements, billboards, text messages and the Internet to propagate anti-extremism views."[151]

Additionally, security agencies have been authorized to block several websites that contain offensive radical religious sites violating "the principles of Islam and social norms."[152] Similarly, the Kingdom has initiated the 'Sakinah' campaign aimed at combating Internet radicalization and recruitment. The program is named after "the Arabic word for religious-inspired tranquility, [and] it operates as an NGO [non-governmental organization] supported by the Ministry of Islamic Affairs."[153]

The introduction of such varied "security measures has driven many dedicated extremists to avoid the Internet and other potentially compromising technologies altogether."[154] As the evidence of the study shows, the Islamic State members utilize the Internet for both propaganda and communication. The Internet is used by the group as a platform to post videos of their crimes for propaganda purposes, as well as for texting messages to each other for communication.

150 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 8.

151Ibid., 30.

152 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 35.

153 Ibid., 36.

154 Ibid.

## D. BANKING AND FINANCIAL LAWS

Saudi Arabia is a party to the Middle East and North Africa Financial Action Task Force, a Financial Action Task Force (FATF)-style regional body; therefore, the Saudi Arabia financial intelligence unit is an important member of the Egmont Group of Financial Intelligence Units.[155] In this capacity, Saudi Arabia makes critical efforts to counter terrorist fundraising and finance activities on Saudi soil. Since the May 12, 2003, attacks in Riyadh, Saudi Arabia has been enforcing strict laws on banking and financial operations across the state, working closely with the United States.[156] As detailed in the following paragraphs, the Kingdom of Saudi Arabia has established the Financial Intelligence Unit responsible for enacting the country's Anti-Money Laundering Law by monitoring wire transfers, transactions, and illicit funds.[157]

### 1. Combating Financing Terrorist Organizations

In ratification of the 'International Convention for the Suppression of the Financing of Terrorism" adopted by the UN General Assembly in December 1999, Saudi Arabia has implemented the mandates strictly by identifying, detecting, freezing, and seizing funds raised to finance terrorism.[158] Therefore, the Saudi "Law Concerning Crimes of Terrorism and its Financing" empowers the Minister of Interior to deal strictly with individuals or organizations suspected of fundraising for or financing terrorist organizations. Financing terrorism, according to Saudi Arabia's law, falls under the crime of *hirabah,* which is defined by Shariah Law:

> For its statutes, the Kingdom of Saudi Arabia relies on Islamic law. The financing of terrorism falls into the category of "spreading evil on earth" (al-ifsad fi al-ard). This may incur the non-discretionary

155Gary Youinou, "Saudi Arabia, Risk & Compliance," Know Your Country, December 2014, 15, http://www.knowyourcountry.com/files/saudiarabiaaug14_2_.pdf.

156 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 13.

157 Ibid., 23.

158 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 22.

> hadd penalty for hirabah (brigandage), which can sometimes mean the application of the death penalty.[159]

As terror networks engage in illicit fundraising under the umbrella of charitable organizations, Saudi Arabia has implemented strict financial control systems to block this activity. These include prohibiting charity organizations from transferring money abroad.[160] Additionally, the Saudi government has prohibited "collection of cash contributions in mosques and public places as a practice of zakat."[161] Furthermore, Saudi Arabia has intensified control over the "cash smuggling from individual donors and charities [engaged in] terrorist financing."[162] Gary Youinou in his report on Saudi Arabia's risk and compliance asserts:

> Saudi Arabia's Council of Senior Scholars (the Kingdom's highest judicial body and equivalent to the U.S. Supreme Court) issued an edict (fatwa) declaring that financing terrorism, knowingly or unknowingly, was illegal and punishable under Islamic law. Separately, in late 2013, Saudi Arabia ratified a new antiterrorism law that criminalizes any act "which includes raising money, offering, taking, allocating, transporting, transferring it—or its revenues—in whole or in part, for any individual or group terrorist activity."[163]

### 2. Combating Money Laundering by Terrorists

Prior to the September 11, 2001 attacks, there was a network of terrorist-financing money transfer centers across the Saudi state. These centers used to finance terrorists hiding behind "charities."[164] After the attacks on the United States, Saudi Arabia increased its crackdown on these organizations, responding to repeated allegations that they were financing terrorism. The Saudi state has

159 The Law Library of Congress," Algeria, Morocco, Saudi Arabia: Response to Terrorism,"6.

160 Celina B. Realuyo, *Combating Terrorist Financing in the Gulf: Significant Progress but Risks Remain*, Arab Gulf States in Washington, January 26, 2015, 9,www.agsiw.org/wp-content/uploads/2015/01/AGSIW_Combating-Terrorist-Financing-in-the-Gulf.pdf.

161 Ibid.

162 Ibid.

163 Youinou," Saudi Arabia, Risk & Compliance," 10.

164 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 25.

established the High Commission for Oversight of Charities as a reform measure focused on Saudi charities.[165] Additionally, the Kingdom has initiated the Saudi Arabia Anti-Money Laundering Law to control such transactions and transfers of illicit funds.[166]

The Anti-Money Laundering Law empowers security agencies to investigate any suspicious financial transactions and to prohibit financial institutions from engaging in or entering into any financial or commercial transactions, or any operations connected with anonymous or fictitious names or numbered accounts.[167] The law further requires "the identity and legal status of the customers and real beneficiaries shall be verified, based on official documents effective at the beginning of the transactions."[168] Financial institutions are also required to report and update the Saudi authorities with all transactions regularly.[169] Furthermore, the Saudi Arabia's Monetary Agency (SAMA) has implemented training programs aimed to "train judges and investigators on legal matters involving terrorism financing and money laundering methods."[170]

165 Ibid.

166 Ibid., 23.

167 Saudi Arabia, Saudi Arabian Monetary Agency, *Anti-Money Laundering and Counter-Terrorism Financing Rules For Financing Companies*, Banking Inspection Department, February 2012, 6, http://www.sama.gov.sa/en-US/Laws/BankingRules/Anti-Money_Laundering_and_Counter-Terrorism_Financing_Rules_For_Financing_Companies.pdf.

168 Ibid., 6.

169 Ibid.

170 Realuyo, *Combating Terrorist Financing in the Gulf*, 9.

# IV. EXPLAINING SAUDI ARABIA'S COUNTERTERRORISM RESPONSES

Terrorist groups such as the Islamic State refer to Saudi Arabia as Wilayat al Haramayn, which means the Province of the Two Holy Places, which are the Islamic holy sites of Mecca and Medina.[171] Occupying Mecca and Medina offers a way for the Islamic State to gain legitimacy. Therefore, the Islamic State, and Al Qaeda prior to it, targeted the Saudi soil and intensified their attacks there. Saudi Arabia, on the other hand, has intensified its varied and multidimensional countermeasures to respond to these attacks successfully. To explain the effectiveness of these responses, it is prudent to revisit the three fundamental questions posed in Chapter I. The first one is, what legal, financial, and informational counterterrorism measures does Saudi Arabia use today to respond to Islamic State threats?

The second question is, what countermeasures does Saudi Arabia need to implement to combat the Islamic State's threats? The third one is, what else does Saudi Arabia need to do to foil the Islamic State's plans? The answer to these questions requires introducing the incidents of terrorist attacks on Saudi targets and how Saudi Arabia has successfully responded to them and analyzing these responses within the theoretical framework derived from the literature review on effective counterterrorism measures (provided in Chapter I). These include incidents of suicide bombing, cyber-attacks, and terrorist financing that occurred between 2013 and 2016. By presenting these incidents, this chapter attempts to test how effective Saudi Arabia's strengthened and varied counterterrorism measures, discussed in the previous chapter, would be against such attacks.

171 Gunaratna, "Global Terrorism in 2016," 135.

## A. SAUDI ARABIA'S RESPONSES TO SUICIDE ATTACKS AND SHOOTING INCIDENTS (2013–2016)

The first hypothesis is that Saudi Arabia has most likely enacted stricter criminal laws and enforcement of those laws for safeguarding the homeland and strengthening surveillance of borders and residential territories to prevent terrorist attacks. A vital example for such counterterrorism strategy is that of the United States after the events of September 11, 2001. Following the attacks on its homeland, the U.S. Congress passed strict laws, such as the Aviation and Transportation Security Act, which mandated background checks and screening of all travelers and their luggage, as well as increased border patrol measures.[172] The laws also enabled a national strategy regarding the detection and identification of terrorist activities to prevent attacks and regarding an immediate response to any terrorist attack within the United States. These measures granted security forces the right to detain and investigate individuals suspected of being affiliated with terrorist organizations.[173]

Similarly, the United Kingdom's Terrorism Act 2000 provided the police the authority to arrest suspected individuals and to investigate them "without a warrant based on a reasonable suspicion that they have been involved in the preparation, instigation, or commission of acts of terrorism."[174] Since then, statistical records show that "Asian and black people are respectively four and five times more likely to be stopped than white people under this Act."[175] Thus, such enacting such legislation may have helped the government of the United Kingdom ensure the safety of its citizens, but implementing the law presented

172 Zelman, "Recent Developments in International Law," 4.

173 Ibid., 6,8.

174 Feikert and Doyle, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States,* 1, 2.

175 Ibid., 3.

government officials with the difficult task of doing so while still protecting the citizens' individual rights.[176]

Likewise, since 2003 the Kingdom of Saudi Arabia has adopted a broad range of security and safety measures represented in "domestic security and counterterrorism, civil defense, criminal investigations and counterespionage, prison administration, passports and border security, and infrastructure protection."[177] Such tasks are authorized by new counterterrorism legislation. The legislation criminalizes all deeds that cause public disorder, damage the image of Saudi Arabia, or threaten its national unity.[178] Besides the strictly enforcing the law through arrest and imprisonment, the Kingdom has adopted soft counterterrorism measures represented in prevention, rehabilitation, and aftercare programs.[179] These programs are intended to deter Saudis from involvement in radicalization, offer rehabilitation counseling and means, and provide aftercare programs to individuals involved in radicalization to "facilitate [their] reintegration into society after their release from custody."[180]

Despite such strict measures, throughout the period from 2013 to 2016, Saudi Arabia experienced several attacks from the Islamic State. Table 1 summarizes the attacks carried out by the terrorist group against the Saudi state and responses by Saudi Arabia.

176 Feikert and Doyle, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States*, 5.

177 Boucek, *Saudi Arabia's "Soft" Counter-terrorism Strategy*, 5.

178 The Law Library of Congress, "Algeria, Morocco, Saudi Arabia: Response to Terrorism," 2.

179 Boucek, *Saudi Arabia's "Soft" Counter-terrorism Strategy*, 4.

180 Ibid.

Table 1. Islamic State Shooting Attacks in Saudi Arabia (2013–2016)[181]

| Year | Date | Incident |
|---|---|---|
| 2014 | August 25 | Saudi security forces arrested eight Islamic State commanders. |
| | November 3 | Seven people were injured during a shooting at a mosque in al-Dalwa in the Eastern Province. |
| | November 22 | A Danish citizen was killed in Riyadh. |
| | January 5 | Four militants and three security forces including a Saudi general were killed at the 'Judayat Aran' border post near Iraq. |
| 2015 | March 29 | Some militants attacked a security patrol in Western Riyadh injuring two. |
| | April 8 | Some militants attacked a security patrol in Eastern Riyadh killing two. |
| | May 8 | Some militants attacked a security patrol south of Riyadh killing one. |
| | May 22 | A suicide bomber attacked Ali bin Abi Talib mosque in al-Qudeih village, Qatif governorate, killing 21 people and injuring more than 80. |
| | July 4 | Saudi security forces raid in Taif resulted in the killing of an officer and a militant, and the arrest of three militants. |
| | July 14 | Saudi security forces raid near Abha resulted in the killing of a militant and his father, injuring two other individuals. |
| | September 23 | Two militants killed a relative in the security forces, two civilians and a police officer. |
| | September 26 | Saudi security forces killed two militants. |
| 2016 | January 28 | 33 militants were arrested by Saudi security forces. Among the group were nine Americans and three Yemenis. |
| | February 15 | Some militants killed a retired Saudi security official in Jizan Province. |
| | April | Some militants killed a senior Saudi security officer in al-Dawami district. |

As the figures in Table 1 show, 2015 witnessed the largest number of shooting attacks by the Islamic State on Saudi targets, while 2014 and 2016 show fewer attacks and no cases reported in 2013. In 2014, the Saudi government jailed 800 people affiliated with the Islamic State.[182] Similarly, in 2015, the Saudi security forces arrested more than 1,300 Saudi nationals and over "300 foreigners on suspicion of connection to the Daesh/ISIL organization."[183] Saudi security forces' firm response to domestic security threats

181 Adapted from 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 67, 68, 69.

182 Ibid., 47.

183 Ibid.

is very typical and aligns with the first hypothesized strategy of counterterrorism, which is enacting strict criminal law and enforcing that law by arresting terrorists and preventing them from carrying out attacks on Saudi targets. On such grounds, the study includes the first hypothesis of Saudi Arabia's implementation of strict criminal law enforcement that includes safeguarding the homeland, surveillance of borders and residential territories to prevent terrorists' attack.

As the figures in Table 2 show, 2015 witnessed the largest number of Islamic State suicide attacks on Saudi targets. By contrast, 2016 shows fewer attacks and no cases reported in 2013 and 2014. If not the strict surety measures, such attacks could have increased. It is also remarkable that most of the suicide incidents target Shiite mosques and security forces. In terms of targeting Shiite mosques, the ISIS aims to provoke Sunni Muslims against Shiite while it classifies security forces as infidels who protect infidel rulers.

Table 2. Islamic State Suicide Attacks in Saudi Arabia (2013–2016)[184]

| Year | Date | Incident |
|---|---|---|
| 2015 | May 22 | A suicide bomber attacked Ali bin Abi Talib mosque in al-Qudeih village, Qatif governorate, killing 21 people and injuring more than 80. |
| | May 29 | A suicide bomber killed four people near Imam Hussain mosque in Dammam. |
| | July 16 | A militant murdered a relative in the security forces, and then injured two people with a suicide bomb detonated at a checkpoint in Riyadh. |
| | August 6 | A suicide bomb at the Saudi Emergency Forces mosque in Asir killed 15 people and injuring 33 others. |
| | October 26 | A suicide bomber killed two, injuring many others in a Shi'ite Ismaili mosque in Najran. |
| 2016 | February 8 | A car bomb explosion targeted some Saudi armed forces in the Al-Azizyah district of Riyadh. |

## B. SAUDI ARABIA'S RESPONSES TO CYBER-ATTACKS (2013–2016)

The second hypothesis is that Saudi Arabia most likely implemented strict cybersecurity measures to monitor terrorist communications and foil their plans.

[184] Adapted from 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," Chapter IV, 68, 69.

The United States, for instance, after September 11, 2001, imposed a strict National Cybersecurity Protection System, the NCPP, working "collaboratively with public, private, and international entities to protect infrastructure, enhance situational awareness and implement analysis, warning and risk-management programs."[185] This system effectively blocks all malicious attempts to access the computer networks and sensitive data within "federal executive branch civilian agencies while working closely with those agencies to bolster their defensive capabilities."186

The United Kingdom, on the other hand, imposed a variety of methods "supported by the National Cyber Security Program (NCSP), with dedicated funding of £860 million."187 The program supports "a wide range of projects to develop cyber security capabilities and stimulate the UK's cyber security market."[188] For instance, the government launched to a campaign that raises awareness among businesses "of the threat from cybercrime and espionage and encourage[s] firms to embed effective cyber security risk management practices."[189] While the NCSP protects businesses and organizations, the DCPP has been initiated "to improve cyber security within the defense supply chain, and continues to focus on best practices, awareness, and proportionate standards."[190]

The Kingdom of Saudi Arabia, likewise, has approved the Anti-cyber-crime Law, which addresses electronic crimes such as "credit card fraud, Internet crimes, cyber terrorism, creation and/or distribution of viruses, hacking, system

185 U.S. Department of Homeland Security, "Safeguarding and Securing Cyberspace."

186 Ibid.

187 The United Kingdom, Cabinet Office, *The UK Cyber Security Strategy, Report on Progress and Forward Plans,* 2.

188 Ibid.

189 Ibid., 3.

190 The United Kingdom, Cabinet Office, *The UK Cyber Security Strategy, Report on Progress and Forward Plans,* 15.

interference, illegal access and interception."[191] Violators have faced heavy penalties ranging from imprisonment to fines. Furthermore, Saudi Arabia has invested heavily in enhancing it cyber capabilities to surpass those of any country in the Middle East.

In cooperation with the Ministry of Defense, the government has formed a unified department to deal with "both the public and private sector, [and] specifically tasked to defend the Kingdom against cyber threats."[192] The following tables summarize Islamic State cyber-attacks in Saudi Arabia and how Saudi Arabia responded to them.

### 1. Terrorist Cyber-Crimes of Sabotage (2013–2016)

As the data in Table 3 show, most of the cyber-attacks that target the Kingdom of Saudi Arabia are strongly connected to the Islamic State. The Syrian Electronic Army and the Cyber of Emotion Team, are no doubt sponsored by the Islamic State to undermine Saudi Arabia's cybersecurity as the Islamic State has claimed on its website.

191 Elnaim, "Cyber Crime in Kingdom of Saudi Arabia," 16.

192 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 8.

Table 3. Islamic State's Cyber-Attacks in Saudi Arabia (2013–2016)

| Year | Date | Incident | Perpetrator |
|---|---|---|---|
| 2013 | May | Several government websites in Saudi Arabia were hacked in a series of heavy cyber-attacks.[193] | Syrian Electronic Army |
| 2015 | August | More than 24 Saudi government websites were briefly hacked.[194] | Cyber of Emotion Team |
| | July | The Islamic State attacked a Saudi Arabian government computer network (database?) and published a list containing employees' data, including their names, phone numbers, and email addresses.[195] | United Cyber Caliphate |

### 2. Terrorist Cyber-Crimes as Propaganda (2013–2016)

To foil the increasing number of terrorist cyber threats, Saudi Arabia has intensified its efforts to intercept wireless communications and monitor social media utilized for terrorist activities.[196] A prime example of this is the arrest of Sayed Zabiuddin Ansari, who is also known as Abu Jundal, by Saudi security forces in 2012, who then handed him over to the Indian authorities.[197] Abu

193 Al Jazeera, "Hackers Target Saudi Government Websites State News Agency Says "Coordinated and Simultaneous" Attacks Traced to IP Addresses from a Number of Countries.," *Aljazeera*, May 17, 2013, http://www.aljazeera.com/news/middleeast/2013/05/201351717324639258 9.html.

194 Al Jazeera, "Saudi Websites Hacked by 'Well-intentioned' Group: More than 24 Government Websites Briefly Hacked by Group that Said It Wanted to Warn Administrators over Cybersecurity," *Al Jazeera*, August 15, 2015, http://www.aljazeera.com/news/2015/08/saudi-websites-hacked-intentioned-group-150815194012877.html.

195 SITE Intelligence Group, *United Cyber Caliphate Claim to Release Saudi Government Employee Data,* July 3, 2016,

https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=745&Itemid=1355.

196 The Law Library of Congress, "Algeria, Morocco, Saudi Arabia: Response to Terrorism," 6.

197 Manoharan, "Abu Jundal's Arrest and India-Saudi Arabia Counter-terrorism Cooperation," Vivekananda International Foundation, July 6, 2012, http://www.vifindia.org/article/2012/july/06/abu-jundal-s-arrest-and-india-saudi-arabia-counter-terrorism-cooperation.

Jundal, an Indian national affiliated with the Pakistan Lashkar-e-Toiba (LeT), was "involved in several terror attacks in various parts of India."[198] He was sent to Saudi Arabia by the "LeT to mobilize funds and recruits from Indian Muslims working there."[199] The Saudi security forces successfully arrested him "working on his assignment even by using Internet, especially the social networking site Facebook."[200]

Another incident is the arrest of Yazied Mohammad Abdulrahman Abu Nayan, the perpetrator of April 8, 2015, shooting in the Saudi capital.[201] Nayan was arrested as he was preparing car bombs targeting Saudi Arabia. During the operation, security forces uncovered wireless messages he exchanged with the Islamic State members in Syria, along with "audio and video confirmation of the attack."[202] Similarly, in March 2016, six Saudi cousins pledged allegiance to the Islamic State and killed another cousin Sergeant Bader al-Rashidi, whose tragic killing was released by the group in a shocking video tape.[203]

After the incident, the ringleader, Wael al-Rashidi, who worked as a pharmacist in a Riyadh hospital, addressed the camera in the video threatening Saudi authorities.[204] In response, "Saudi security forces tracked the six men to a remote location and killed them all in a shootout, local news outlets reported."[205] Saudi Arabia's responses to both cyber-attacks and its tracking of wireless communication and social media align with the second hypothesized counter-terrorism strategy. That strategy includes the implementation of intensified cyber-

198 Ibid.

199 Ibid.

200 Ibid.

201 Vice News, "Saudi Arabia Says Gunman Allegedly behind Police Killings Received Instructions from Islamic State," *Vice News*, April 24, 2015, https://news.vice.com/article/saudi-arabia-says-gunman-allegedly-behind-police-killings-received-instructions-from-islamic-state.

202 Ibid.

203 Ben Hubbard, "ISIS Turns Saudis against the Kingdom, and Families against Their Own," *New York Times*, March 31, 2016, https://www.nytimes.com/2016/04/01/world/middleeast/isis-saudi-arabia-wahhabism.html?_r=0.

204 Ibid.

205 Ibid.

security measures. Thus, this case study supports the second hypothesis that Saudi Arabia has implemented strict cybersecurity measures to track terrorist communications and foil their plans.

## C. ILLEGAL FINANCING OF TERRORIST ORGANIZATIONS AND MONEY LAUNDERING IN SAUDI ARABIA (2013–2016)

The third hypothesis is that Saudi Arabia most likely implemented strict banking laws to prevent terrorist fundraising and other financial activities that fund the Islamic State's operation. The United States, for instance, after September 11, 2001, imposed strict laws on banks and financial institutions. These laws prohibit "the maintenance of correspondent accounts for foreign banks that have no physical presence in any country."[206] Furthermore, the banks and financial institutions are required to report suspicious activities and disclose bank records of any financial institution "under investigation for financial crimes related to terrorism."[207] To maintain a stringent counterintelligence investigation, these institutions are required to disclose confidential communications, transaction records, financial reports, and credit information.[208]

In the ratification of the 'International Convention for the Suppression of the Financing of Terrorism" adopted by the UN General Assembly in December 1999, Saudi Arabia similarly implemented the mandates by identifying, detecting, freezing, and seizing funds raised to finance terrorism.[209] The Saudi Banking Law Concerning Crimes of Terrorism and its Financing empowers the Minister of Interior to deal strictly with individuals or organizations suspected of fundraising or financing terrorist organizations.[210] Additionally, the law has prohibited

206 Zelman, "Recent Developments in International Law," 5.

207 Ibid.

208 Ibid., 4.

209 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 22.

210 The Law Library of Congress," Algeria, Morocco, Saudi Arabia: Response to Terrorism," 6.

"collection of cash contributions in mosques and public places as a practice of zakat."[211]

The Anti-Money Laundering Law, on the other hand, empowers security agencies to investigate any suspicious financial transactions and to prohibit financial institutions from engaging in or entering into any financial or commercial transactions or operations connected with anonymous or fictitious names or numbered accounts.[212] To maintain top banking measures, all financial institutions are required to report and update the Saudi authorities with all transactions regularly.[213] The following sections detail terrorist financing and money laundering incidents and how the Saudi authorities responded to them.

### 1. Incidents of Financing Terrorist Organizations (2013–2016)

Despite the frequent terrorist attacks on Saudi targets throughout the period of 2012 to 2016, the Saudi state successfully stopped the financing of terrorist organizations on its soil.[214] This was accomplished by the strong measures Saudi Arabia has pursued to disrupt terrorists franchising on its soil in cooperation with the Counter-ISIL Finance Group, which is led jointly by Italy, Saudi Arabia, and the United States.[215] Prior to this, for instance on October 1, 2013, the Saudi "Specialized Criminal Court in Riyadh convicted a cleric guilty of financing terrorism."[216] The cleric, besides financing terrorism, was also found guilty of "issuing fatwas in support of terrorist suicide operations, and interfering in the affairs of foreign sovereign nations."[217]

---

211 Ibid.

212 Saudi Arabia, Saudi Arabian Monetary Agency,"Anti-Money Laundering and Counter-Terrorism Financing Rules For Financing Companies," 6.

213 Ibid.

214 28pages.org, "The Kingdom of Saudi Arabia and Counter-Terrorism," 13.

215 Ibid., 14.

216 Youinou, "Saudi Arabia, Risk & Compliance," 15, http://www.knowyourcountry.com/files/saudiarabiaaug14_2_.pdf.

217 Ibid.

### 2. Incidents of Money Laundering (2013–2016)

Like the cases of financing terrorist organizations, cases of money laundering on Saudi soil have also almost vanished since 2012 because of the great efforts Saudi Arabia makes to prevent such activities. On June 26, 2012, for instance, the Saudi Specialized Criminal Court sentenced a member of "Khafji cell" to 15 years in prison with an additional 15-year travel ban.[218] The man pleaded "guilty [to] supporting terrorism through money laundering and other crimes, such as possessing unlicensed fire arms."[219]

Since then, terrorist financing and money laundering have almost disappeared. In fact, there are no reported cases being tried in the courts from 2013 up to 2017. In this sense, Saudi Arabia's responses to incidents involving financing of terrorist organizations and money laundering align with the third hypothesized counterterrorism strategy based on implementing intensified financial and banking measures. Thus, the case study supports the hypothesis that Saudi Arabia has implemented strict banking laws to prevent terrorist fundraising and to eliminate financial sources to fund the Islamic State's operation.

218 United States Department of State Bureau of Counterterrorism, *Country Reports on Terrorism 2012*, 139,

219 Ibid.

# V. CONCLUSION AND POLICY IMPLICATIONS

Unlike al-Qaeda's threats, which the Kingdom has been countering since 2003, the Islamic State's threats have driven Saudi Arabia to transform its counterterrorism efforts into a multidimensional approach. This thesis has sought to discern in what ways Saudi Arabia has transformed its countermeasures and whether these methods have been effective. The examples presented in the previous chapter highlight the Kingdom's effective responses to terrorist attacks on Saudi soil. Specifically, these examples answer the major research question regarding what legal, financial, and informational countermeasures Saudi Arabia currently uses and, in this chapter, these examples allow us to answer the question about what can be done to enhance the Kingdom's current countermeasures. Thus, the chapter introduces policy implications that present recommendations for policymakers, and finally, the chapter presents concluding remarks restating the answers of the major research questions.

## A. EVALUATION OF EVIDENCE TESTED AGAINST THE HYPOTHESES

The first chapter presented three major research questions. First, what legal, financial, and informational counterterrorism measures (does Saudi Arabia use today to respond to Islamic State threats? Second, what additional countermeasures—legal, financial, and informational—does Saudi Arabia still need to implement to combat the Islamic State's threats? Third, what else does Saudi Arabia need to do to foil the Islamic State's plans? The thesis has attempted to answer these questions with the following three hypotheses:

> **Hypothesis I:** Saudi Arabia most likely implemented stricter criminal laws and law enforcement, related to safeguarding the homeland and surveilling borders and residential territories to prevent terrorist attacks. This hypothesis is modeled on the legal measures taken by other nations that have been impacted by Islamic State terrorism. A key example for such a counterterrorism strategy is that of the United States after the events of September 11, 2001.[220] Similarly, the United Kingdom's

220 Zelman, "Recent Developments in International Law," 4.

Terrorism Act 2000 provides the police the authority to arrest suspected individuals and investigate them "without a warrant based on a reasonable suspicion that they have been involved in the preparation, instigation, or commission of acts of terrorism."[221]

**Hypothesis II:** Saudi Arabia most likely implemented strict cybersecurity measures to track terrorist communications and foil the Islamic State's plans. This hypothesis, like the first, assumes that the methods adopted by the United States and the United Kingdom are reflected in Saudi Arabia's measures. The United States, for instance, after September 11, 2001, imposed a strict National Cybersecurity Protection System, the National Cybersecurity Protection Plan (NCPP), working "collaboratively with public, private, and international entities to protect infrastructure, enhance situational awareness and implement analysis, warning and risk-management programs."[222] The United Kingdom, on the other hand, imposed a variety of methods "supported by the National Cyber Security Program (NCSP), with dedicated funding of £860 million."[223]

**Hypothesis III:** Saudi Arabia most likely implemented strict banking laws to prevent terrorist fundraising and eliminate illegal sources of income that fund the Islamic State's operation. The United States, for instance, after September 11, 2001, imposed strict laws on banks and financial institutions. These laws prohibited "the maintenance of correspondent accounts for foreign banks that have no physical presence in any country."[224]

These hypotheses were examined in the previous chapter with examples from the case studies related to terrorist attacks and Saudi Arabia's responses. Furthermore, the methods of responding discussed in the third and fourth chapters align with the predicted answers to the major research questions. Each hypothesis introduced in the first chapter fully fits with the evidence discussed in the third and fourth chapters. Specifically, the first hypothesis shows congruence with Saudi Arabia's strict criminal law enforcement response to the Islamic State's suicide and shooting incidents shown in Tables 1 and 2. That response

221 Feikert and Doyle, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States*,1, 2.

222 U.S. Department of Homeland Security, "Safeguarding and Securing Cyberspace."

223 The United Kingdom, Cabinet Office, *The UK Cyber Security Strategy, Report on Progress and Forward Plans*, 2.

224 Zelman, "Recent Developments in International Law," 5.

includes safeguarding the homeland and surveilling borders and residential territories to prevent terrorist attacks.

Similarly, the second hypothesis shows congruence with Saudi Arabia's Anti-cyber-crime Law responses which address electronic crimes such as "credit card frauds, Internet crimes, cyber terrorism, creation and/or distribution of viruses, hacking, system interference, illegal access and interception."[225] A vital example for this, is Saudi Arabia's responses to the sabotage cyber-attacks shown in Table 3 and terrorist cybercrimes for propaganda incidents such as the arrest of Abu Jundal, Abu Nayan, and Wael al-Rashidi.

Likewise, the third hypothesis is congruent with Saudi Arabia's implementation of strict banking laws to prevent terrorist fundraising and eliminate illegal sources of income that fund the Islamic State's operation. These measures are similar to the United States' implementation of strengthened laws on banks and financial institutions after September 11, 2001, which prohibited "the maintenance of correspondent accounts for foreign banks that have no physical presence in any country."[226] For instance, on October 1, 2013, the Saudi "Specialized Criminal Court in Riyadh convicted a cleric guilty of financing terrorism."[227] Similarly, on June 26, 2012, the Saudi Specialized Criminal Court sentenced a member of "Khafji cell" to 15 years in imprison in addition to a 15-year travel ban.[228] The man had been found "guilty of supporting terrorism through money laundering and other crimes, such as possessing unlicensed fire arms."[229]

225 Elnaim, "Cyber Crime in Kingdom of Saudi Arabia," 16.

226 Zelman, "Recent Developments in International Law," 5.

227 Youinou, "Saudi Arabia, Risk & Compliance," 15.

228 United States Department of State Bureau of Counterterrorism, *Country Reports on Terrorism 2012*, 139,

229 Ibid.

Beyond the specific measures used by Saudi Arabia to combat terrorism, which are predicted in the hypotheses themselves, there is still a generalizability question. That is, "Do the previously introduced hypotheses port to other measures?" The answer is of course they do port. Briefly, there is one more strategic measure to be considered, the soft measure strategy. The Saudi Ministry of Interior has initiated non-punitive efforts to rehabilitate citizens convicted of terrorism-related offenses and to prevent the radicalization of vulnerable populations.

The program, as explained in Chapter III, has been adopted by the Kingdom as a non-punitive and soft counterterrorism measure that consists of prevention, rehabilitation, and aftercare programs.[230] These programs aim to deter Saudis from involvement in radicalization, offer rehabilitation counseling and means, and provide aftercare programs to individuals involved in radicalization to "facilitate reintegration into society after their release from custody."[231] This model counterterrorism approach has been very successful and imitated by many other countries, including as Singapore, the United Kingdom, and Denmark.[232] The Saudi government has invested tremendous resources to provide prisoners "ongoing counseling, financial support, and career development assistance after graduation from the program."[233]

Considering these together, the reviews of Saudi Arabia's counterterrorism measures demonstrate that the hypotheses introduced in the first chapter as well as introduce another measure, an effective soft approach. This additional approach expands the multidimensional response that Saudi Arabia implements to combat and deter the Islamic State's threats.

230 Boucek, *Saudi Arabia's "Soft" Counter-terrorism Strategy*, 4.

231 Ibid.

232 Barcena, Daines, and Noh, *Combatting Terrorism Through Prosecutions & Rehabilitation*, 3.

233 Ibid, 25.

## B. POLICY IMPLICATIONS

The purpose of this thesis is to help policymakers better understand Saudi Arabia's current counterterrorism measures and how they are effective. Using this knowledge, policymakers can design measurable counterterrorism methods to eliminate the Islamic State. With many terrorist organizations, such as al-Qaeda and the Taliban, carrying out violent acts regionally and internationally, a range of measures have been deployed to counter and defeat them in the past few years. These measures have included international cooperation, diplomacy, constructive engagement, protective security measures, economic sanctions, covert action, and military force.[234] Among these approaches, military intervention followed by regime change has been frequently used; nevertheless, each of the measures has its cons and pros as demonstrated. The following paragraphs offer recommendations for policymakers to develop new approaches and enhance existing ones.

### 1. Recommendation I: Sanctions on Islamic State Members and Entities

To choke the revenue streams that enable terrorist operations, for example, the United States and others have implemented economic sanctions. President Bush signed Executive Order 13224 on September 23, 2001, "freezing the assets of 27 individuals and organizations known to be affiliated with bin Laden's network."[235] This freeze list was later "expanded to include designated terrorist groups, supporters, and financiers of terror."[236] The UN Security Council, on the other hand, implemented Resolution 1373 on January 16, 2002, obligating "member states to freeze funds of 'individuals, groups, undertakings, and entities'

234 Raphael F. Perl, *International Terrorism: Threat, Policy, and Response* (CRS Report No. RL33600) (Washington, DC: Congressional Research Service, 2007), 9, http://fas.org/sgp/crs/terror/RL33600.pdf.

235 Ibid., 14

236 Ibid.

associated with the Taliban and Al Qaeda."[237] Such measure was very effective tool to limit the financial capabilities of the organization.

Unlike al-Qaeda, the Islamic State possesses a more sophisticated financial system and varied resources. The UN Security Council has adopted a number of "resolutions against ISIS, for the most part concerning financial sanctions."[238] Resolution 2253, of December 17, 2015, for instance, "extends to Islamic State the sanctions regime" adopted against Al Qaeda, calling upon states to "criminalize financial transactions related to terrorism," designing guidance to destroy the mechanisms of ISIS financing such as "oil smuggling, extortion and taxation, robbery, kidnapping for ransom, foreign donations, trade in antiquities, and human trafficking."[239]

Additionally, the resolution requests states to improve information sharing by implementing "the international standards and guidelines developed by FATF."[240] Beyond sharing information, other resolutions direct member states to take aim at sources of terrorist funding. Resolution 2170 of 2014, for example, "condemns all commercial transactions undertaken with terrorist groups, including ISIS, especially in the oil sector."[241] In February 2015 the UN Security Council adopted Resolution 2199 calling upon "the member states to cut off the sources of ISIS financing."[242] Yet, the Islamic State still efficiently generates income for the organization; therefore, Saudi Arabia and its partners are strongly recommended to pursue coercive penalties for individuals or states that are not fully cooperative with the resolutions.

237Perl, *International Terrorism: Threat, Policy, and Response*, 14.

238 Bindner and Poirot, "ISIS Financing 2015," 26.

239 Ibid.

240 Ibid.

241 Ibid.

242 Ibid.

### 2. Recommendation II: Military Intervention and Regime Change in Syria

Changing the Al-Asaad regime in Syria will help the International Alliance to root out and end the Islamic State's threats to Saudia Arabia and its partners. Military intervention and regime change such as in Iraq, and Libya, and Afghanistan, targeting the Taliban and its supporters, are decisive measures to root out policymakers who enable terrorism. After the al-Qaeda attacks of September 11, 2001, the United States and its partners invaded Afghanistan and ousted the Taliban regime, which was hosting and supporting al-Qaeda.[243] Despite the fruitful outcome of the invasion, though, such measures have often yielded more violence and extremism. For instance, since the collapse of the Taliban regime, Afghanistan has become even more insecure and a center for terrorism similar to Iraq, and in Libya regime change has given birth to Ansar al-Sharia, al-Qaeda-affiliates, the Islamic State, and other militias.[244] Yet, Saudi Arabia and its partners are strongly recommended to consider this measure seriously and proceed to change the regime in Syria. To avoid the emergence of other terrorist organizations in the power vacuum that could exist after regime change such as the situation in Libya, Syria should be placed on international mandate until there is a strong government.

### 3. Recommendation III: Destroying the Islamic State's Infrastructure

As mentioned in Chapter II, the Islamic State possesses varied sources of income that enable it to establish a statehood infrastructure. It provides social services, free healthcare to its population, high salaries, and services its fighters even though a significant portion of this infrastructure has suffered severe destruction resulting from the International Alliance's airstrikes.[245] Since 2015

243 Daniel Byman, *Deadly Connections: States That Sponsor Terrorism* (New York: Cambridge University Press, 2005), 194.

244 Jakkie Cilliers, "Violent Islamist Extremism and Terror in Africa," Institute for Security Studies in Africa Issue Brief No. 286, October 2015, 13, 14, https://issafrica.org/uploads/Paper286-1.pdf.

245 Ibid. ??

coalition fighters have intensified heavy airstrikes on all vital targets causing a severe impact on Islamic State revenue sources, such as means of transport, refineries, and oil pipelines, as well as high ranking members of the organization.[246] Nonetheless, these strikes have not yet caused total destruction to the organization's resources and infrastructure. Therefore, Saudi Arabia and its partners are strongly recommended to pursue heavy attacks with ground troops supported by airstrikes targeting members and financial sources of the organization.

## C. CONCLUSION

The first chapter introduced three major research questions. First, what legal, financial, and informational counterterrorism measures (does Saudi Arabia use today to respond to Islamic State threats? Second, what additional countermeasures—legal, financial, and informational—does Saudi Arabia still need to implement to combat the Islamic State's threats? Third, what else does Saudi Arabia need to do to foil the Islamic State's plans? The answer to these questions has required introducing the incidents of terrorist attacks on Saudi targets and how Saudi Arabia has successfully responded to them and analyzing these responses within the theoretical framework derived from the literature review on effective counterterrorism measures (provided in Chapter I). Such incidents have included suicide bombing, cyber-attacks, and terrorist financing that took place between 2013 and 2016. By presenting these incidents, the thesis has tested how effective Saudi Arabia's strengthened and varied counterterrorism measures.

The result is that similar to the United States and the United Kingdom, Saudi Arabia implements strict criminal law enforcement that includes safeguarding the homeland, surveillance of borders and residential territories to prevent terrorists' attack. Since the events of September 11, 2001, the United States, implements strict laws on aviation and transportation represented in

246 Ibid. ???

background checks and screening to travelers and their luggage, as well as increased border patrol measures.[247] Likewise, the United Kingdom since 2000, implements strict laws that provide the police the right of arresting suspected individuals and investigating them "without a warrant based on a reasonable suspicion that they have been involved in the preparation, instigation, or commission of acts of terrorism."[248]

Second, Saudi Arabia implements strict cybersecurity measures to track terrorist communications and foil their plans similar to the United States after the events of September 11, 2001. Since such terrible events, the United States imposes strict represented in the National Cybersecurity Protection System, the NCPP working "collaboratively with public, private, and international entities to protect infrastructure, enhance situational awareness and implement analysis, warning and risk-management programs."[249] The United Kingdom likewise, imposes a variety of methods supported by the NCSP.[250] Third, Saudi Arabia implements strict banking laws to prevent terrorist fundraising and generating finance to fund the Islamic State's operation on the way the United States imposes strict laws on banks and financial institutions since September 11, 2001. Such laws prohibited "the maintenance of correspondent accounts for foreign banks that have no physical presence in any country."[251]

Beyond the specific measures used by Saudi Arabia to combat the Islamic State, evidence has shown that Saudi Arabia pursues non-punitive efforts to rehabilitate citizens convicted of terrorism-related offenses. These programs are established to deter Saudis from involvement in radicalization, offer rehabilitation counseling and means, and provide aftercare programs to individuals involved in

247 Zelman, "Recent Developments in International Law," 1.

248 Feikert and Doyle, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States*,1, 2.

249 U.S. Department of Homeland Security t, "Safeguarding and Securing Cyberspace."

250 The United Kingdom, Cabinet Office, *The UK Cyber Security Strategy, Report on Progress and Forward Plans*, 2.

251 Zelman, "Recent Developments in International Law," 5.

radicalization to “facilitate reintegration into society after their release from custody.”[252] The Saudi government has invested tremendous resources to provide prisoners “ongoing counseling, financial support, and career development assistance after graduation from the program.”[253]

252 Ibid.

253 Ibid, 25.

# LIST OF REFERENCES


28Pages.org. “The Kingdom of Saudi Arabia and Counter-Terrorism.” April 4, 2016. https://28pagesdotorg.files.wordpress.com/2016/05/saudi-lobby-white-paper.pdf.

Al Jazeera. “Hackers Target Saudi Government Websites State News Agency Says ‘Coordinated and Simultaneous’ Attacks Traced to IP Addresses from a Number of Countries.” May 17, 2013. http://www.aljazeera.com/news/middleeast/2013/05/201351717324639258 9.html.

———. “Saudi Websites Hacked by ‘Well-Intentioned’ Group: More than 24 Government Websites Briefly Hacked by Group that Said It Wanted to Warn Administrators over Cybersecurity.” August 15, 2015. http://www.aljazeera.com/news/2015/08/saudi-websites-hacked-intentioned-group-150815194012877.html.

Al-Hadlaq, Abdulrahaman. “Terrorist Rehabilitation: The Saudi Experience.” In *Terrorist Rehabilitation and Counter-Radicalization: New Approaches to Counter-Terrorism*, 60–69. New York: Routledge, 2011. https://books.google.com/books?id=1fWrAgAAQBAJ&pg=PA68&lpg=PA68&dq=CounterTerrorism+from+Within:+Assessing+Saudi+Arabia%27s+Religious+Rehabilitation+and+Disengagement+Programme+pdf&source=bl&ots=JwHaXUDhiU&sig=caTkZeg0M4kruSMEHBKUtfUUTM&hl=en&sa=X&ved=0ahUKEwiTvsz579HRAhUlqFQKHZ62A80Q6AEIITAB#v=onepage&q=Counter-Terrorism%20from%20Within%3A%20Assessing%20Saudi%20Arabia’s%20Religious%20Rehabilitation%20and%20Disengagement%20Programme%20pdf&f=false.

Amnesty International. *Encryption: A Matter of Human Rights.* Report. March 2016. https://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

Azoulay, Rivka. *Islamic State Franchising Tribes, Transnational Jihadi Networks and Generational Shifts.* CRU Report. April 2015. www.clingendael.nl/sites/default/files/Rivka Azoulay_Islamic_State_expansion_CRU_April2015.pdf.

Baitalmal, Hamza A. “Conceptual Framework of Saudi Arabia’s Efforts in Countering Terrorism: The Case of Intellectuals and Mass Media.” Harvard University, 2016. http://scholar.harvard.edu/majidrafizadeh/BaitalmalSAEfforts.

Barcena, Johann Carlos, Kenneth Daines, and John Noh. *Combatting Terrorism through Prosecutions & Rehabilitation: Three Models Compared, A Report to the Bureau of Conflict & Stabilization Operations U.S. Department of State.* Stanford Law School, June 2015. https://law.stanford.edu/publications/combating-terrorism-through-prosecutions-rehabilitation-three-models-compared-a-report-to-the-bureau-of-conflict-stabilization-operations-u-s-department-of-state/.

Bindner, Laurence, and Gabriel Poirot. "ISIS Financing 2015." Center for the Analysis of Terrorism. May 2015. http://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf.

Blanchard, Christopher M., and Carla E. Humud. *The Islamic State and U.S. Policy, Congressional Research Service 7–5700* (CRS Report No. R43612). Washington, DC: Congressional Research Service, February 9, 2016. https://fas.org/sgp/crs/mideast/R43612.pdf.

Boucek, Christopher. “Counter-Terrorism from Within: Assessing Saudi Arabia’s Religious Rehabilitation and Disengagement Programme.” *RUSI* 135, no. 6 (December 19, 2008): 60–65. http://carnegieendowment.org/files/boucek_rusi.pdf.

———. *Saudi Arabia’s “Soft” Counter-terrorism Strategy: Prevention, Rehabilitation, and Aftercare.* Carnegie Endowment for International Peace, Middle East Program*.* Report no. 97. September 2008. http://carnegieendowment.org/files/cp97_boucek_saudi_final.pdf.

Byman, Daniel. *Deadly Connections: States That Sponsor Terrorism*. New York: Cambridge University Press, 2005. https://journals.lib.unb.ca/index.php/jcs/article/view/4517/5332.

———. :The U.S.-Saudi Arabia Counterterrorism Relationship.” Pepared Testimony, Brookings, May 24, 2016. https://www.brookings.edu/wp-content/uploads/2016/07/Byman-Saudi-Arabia-HFAC.pdf.

Cilliers, Jakkie. *Violent Islamist Extremism and Terror in Africa.* Institute for Security Studies in Africa Issue Brief No. 286. October 2015. https://issafrica.org/uploads/Paper286-1.pdf.

Cordesman, Anthony H. *Saudi Arabia and 9/11: Establishing the Truth behind the Release of the 28 Pages and the “Justice against Sponsors of Terrorism Act.”* Washington, DC: Center for Strategic & International Studies, September 14, 2016. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160914_Saudi%20_28_pages_911_Report.pdf.

Eisenstadt, Michael. “Iran’s Lengthening Cyber Shadow.” *Research Notes* 34 (July 24, 2016): 1–19. http://www.washingtoninstitute.org/uploads/Documents/pubs/ResearchNote34_Eisenstadt.pdf.

Elnaim, Bushra Mohamed Elamin. “Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future.” *Information and Knowledge Management (IISTE)* 3, no. 13 (2013): 14–19. http://docplayer.net/15920297-Information-and-knowledge-management-issn-2224-5758-paper-issn-2224-896x-online-vol-3-no-12-2013.html.

Falcone, Robert. “Second Wave of Shamoon 2 Attacks Identified.” Paloalto Network, January 9, 2017. http://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/?__hstc=67007217.dfbe03a820b4634fff1f3b6349592f70.1484912948051.1484912948051.1484912948051.1&__hssc=67007217.1.1484912948053&__hsfp=3179728420.

Feikert, Clare, and Charles Doyle. *Anti-Terrorism Authority under the Laws of the United Kingdom and the United States* (CRS Report No. RL33726). Washington, DC: Congressional Report Service, September 7, 2006. https://www.fas.org/sgp/crs/intel/RL33726.pdf.

Fidler, David P. *Countering Islamic State Exploitation of the Internet.* Digital and Cyberspace Policy Program Cyber Brief. June 2015. http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-Internet/p36644.

The Financial Action Task Force. *Emerging Terrorist Financing Risks*. October 2015. www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.

Finklea, Kristin, Richard M. Thompson II, and Chris Jaikaran. *Court-Ordered Access to Smart Phones: In Brief* (CRS Report No. R44396). Washington, DC: Congressional Research Service, February 23, 2016. https://www.fas.org/sgp/crs/misc/R44396.pdf.

Friedland, Elliot. *The Islamic State*. May 10, 2015. https://www.clarionproject.org/sites/default/files/islamic-state-isis-isil-factsheet-1.pdf.

Gambhir, Harleen. *ISIS Global Strategy: A Wargame.* Middle East Security Studies Report No. 28. Institute for the Study of War. July 2015. http://understandingwar.org/sites/default/files/ISIS%20Global%20Strategy%20--%20A%20Wargame%20FINAL.pdf.

Gunaratna, Rohan. “Global Terrorism in 2016.” *UNISCI Journal* 40 (January 2016): 133–38. https://www.ucm.es/data/cont/media/www/pag-78913/UNISCIDP40-8RohanGunaratna.pdf.

Hoeft, Gabriel. "'Soft' Approaches to Counter-Terrorism: An Exploration of the Benefits of Deradicalization Programs." International Institute for Counter-Terrorism (ICT), Spring 2015, 1–66. https://www.ict.org.il/UserFiles/ICT-Soft-Approaches-to-CT-Hoeft.pdf.

Hoffman, Adam, and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." Institute for National Security Studies, March 20, 2015. http://www.inss.org.il/uploadImages/systemFiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf.

Hubbard, Ben. "ISIS Turns Saudis against the Kingdom, and Families against Their Own." *New York Times*, March 31, 2016. https://www.nytimes.com/2016/04/01/world/middleeast/isis-saudi-arabia-wahhabism.html?_r=0.

Humud, Carla E., Robert Pirog, and Liana Rosen. *Islamic State Financing and U.S. Policy Approaches* (CRS Report No. R43980). Washington, DC: Congressional Research Service, April 10, 2015. https://www.fas.org/sgp/crs/terror/R43980.pdf.

Law Library of Congress. "Algeria, Morocco, Saudi Arabia: Response to Terrorism." Accessed May 1, 2017. https://www.loc.gov/law/help/counterterrorism/response-to-terrorism.pdf.

Lennon, Mike. "ISIS Cyber Capabilities Weak, Poorly Organized: Report." Security Week, April 28, 2016. http://www.securityweek.com/isis-cyber-capabilities-weak-poorly-organized-report.

Manoharan, N. "Abu Jundal's Arrest and India-Saudi Arabia Counter-terrorism Cooperation." Vivekananda International Foundation. July 6, 2012. http://www.vifindia.org/article/2012/july/06/abu-jundal-s-arrest-and-india-saudi-arabia-counter-terrorism-cooperation.

Mohammed Bin Naif Counseling and Care Center. Media Center. "UN Rights Official Commends Saudi Prison Conditions." News release, April 19, 2017. https://www.moi.gov.sa/wps/portal/!ut/p/z1/rVNLU8IwEL7zK-qBYyePpq9jYRAEtdiK0Fw6MWQgDk15VNB_bzqMM0KFwugeNq9vH_l2F9CGYTQaYKIXvfmpDg6AKraVM1bIXLEFmICEOim8I6SHCB5AYnVgYLut56dhH8E2AeMjgB21YeA4oy5xIkjuEaAX2Z-QAF5o_w0IB6GrAa3H_q0_RDC0r7Q_Alj23-J3a-1fAAWUq2JZzEGSMamakOfvaiMWUs0MLlQh1k24f1Bit9lrg635XG6FfuGcp-VVij0TIRND5LBUqNLtkssp SIQnIOFTZrrM903i-7bJbIZNC3H8yrGDLcxraNB50vNV6h_-s1qGcZlQDd NnfXQrgF96rS7N8yECG8SauURz4Z5KNHQQGG-l2IGRyteZHpH4S qp7FbaqbOuxk2-rFQ10b-S6BT4KMPnP5lhmo1Iyz_o046gTeQ8di9D k5gsshTBj/dz/d5/L2dBISEvZ0FBIS9nQSEh/.

Normark, Magnus, and Magnus Ranstorp. *Understanding Terrorist Finance, Modus Operandi and National CTF Regimes.* Report no. 46. December 18, 2015. http://www.fi.se/upload/43_Utredningar/20_Rapporter/2016/Understanding_Terrorist_Finance_160315.pdf.

Paganini, Pierluigi. “Cyber Caliphate Hacks 54k Twitter Accounts, including Ones of CIA and FBI Officials.”*Covai Post*, November 15, 2015. http://www.covaipost.com/aroundtheweb/cyber-caliphate-hacks-54k-twitter-accounts-including-ones-of-cia-and-fbi-officials/.

Perl, Raphael F. *International Terrorism: Threat, Policy, and Response.* January 3, 2007. http://fas.org/sgp/crs/terror/RL33600.pdf.

Realuyo, Celina B. *Combating Terrorist Financing in the Gulf: Significant Progress but Risks Remain.* January 26, 2015. ww.agsiw.org/wp-content/uploads/2015/01/AGSIW_Combating-Terrorist-Financing-in-the-Gulf.pdf.

Riley, Michael, Glen Carey, and John Fraher. “Destructive Hacks Strike Saudi Arabia, Posing Challenge to Trump.” *Bloomberg Technology*, December 1, 2016. https://www.bloomberg.com/news/articles/2016-12-01/destructive-hacks-strike-saudi-arabia-posing-challenge-to-trump.

Roul, Animesh. “India Faces Up to Growing Islamic State Threat.” *Terrorism Monitor* 13, no. 17 (August 21, 2015). http://www.jamestown.org/programs/tm/single/?tx_ttnews%5Btt_news%5D=44304&cHash=dd1d2131cc62a72e28e690f87937a9e4.

Saudi Arabian Monetary Agency, Banking Inspection Department. *Anti-money Laundering and Counter-Terrorism Financing Rules for Financing Companies.* February 2012. http://www.sama.gov.sa/en-US/Laws/BankingRules/Anti-Money_Laundering_and_Counter-Terrorism_Financing_Rules_For_Financing_Companies.pdf.

Siboni, Gabi. “The Military Power of the Islamic State.” Institute for National Security Studies. September 14, 2016. http://www.inss.org.il/index.aspx?id=4538&articleid=11166.

SITE Intelligence Group. *United Cyber Caliphate Claim to Release Saudi Government Employee Data*. July 3, 2016. https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=745&Itemid=1355.

Smith II, Michael S. “Social Media Jihad.” Speech, NC-SC Counterterrorism Conference, National Sheriff’s Association, North Charleston, South Carolina, February 15, 2016. http://kronosadvisory.com/NC.SC.CT.Conf.SocialMediaJihadPresentationRemarks.pdf.

Svanadze, Vladimer. *New Challenges for the Georgian Cyberspace.* Publication no. 52. November 10, 2016. http://gfsis.org/files/library/opinion-papers/52-expert-opinion-eng.pdf.

Technical Analysis Group. *Examining the Cyber Capabilities of Islamic Terrorist Groups*. Institute for Security Technology Studies at Dartmouth College, November 2003. http://www.ists.dartmouth.edu/library/164.pdf.

The United Kingdom, Cabinet Office. *The UK Cyber Security Strategy, Report on Progress and Forward Plans.* December 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

United States Committee on Financial Services. *Task Force to Investigate Terrorism Financing Hearing Entitled "A Survey of Global Terrorism and Terrorist Financing."* U.S. House of Representatives, April 22, 2015. http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=398891.

U.S. Department of Homeland Security. "Safeguarding and Securing Cyberspace." January 19, 2016. https://www.dhs.gov/safeguarding-and-securing-cyberspace.

United States Department of State Bureau of Counterterrorism. *Country Reports on Terrorism 2012.* May 2013. http://www.cardozolawreview.com/content/Symposium/Country%20Reports%20on%20Terrorism%202012.pdf.

———. *Country Reports on Terrorism 2014.* June 2015. https://www.state.gov/documents/organization/239631.pdf.

Vice News. "Saudi Arabia Says Gunman Allegedly behind Police Killings Received Instructions from Islamic State." *Vice News*, April 24, 2015. https://news.vice.com/article/saudi-arabia-says-gunman-allegedly-behind-police-killings-received-instructions-from-islamic-state.

Youinou, Gary. "Saudi Arabia, Risk & Compliance*."* Know Your Country. December 2014. http://www.knowyourcountry.com/files/saudiarabiaaug14_2_.pdf.

Zelin, Aaron Y. *The Saudi Foreign Fighter Presence in Syria.* Washington Institute Report no. 7, Issue 4. April 2014. www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20140428-CTCSentinel.pdf.

Zelman, Joshua D. “Recent Developments in International Law: Anti-Terrorism-Part One: An Overview.” *Journal of Transnational Law and Policy*, 1st ser., 11 (Fall 2001). http://law-wss-01.law.fsu.edu/journals/transnational/vol11_1/zelman.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California